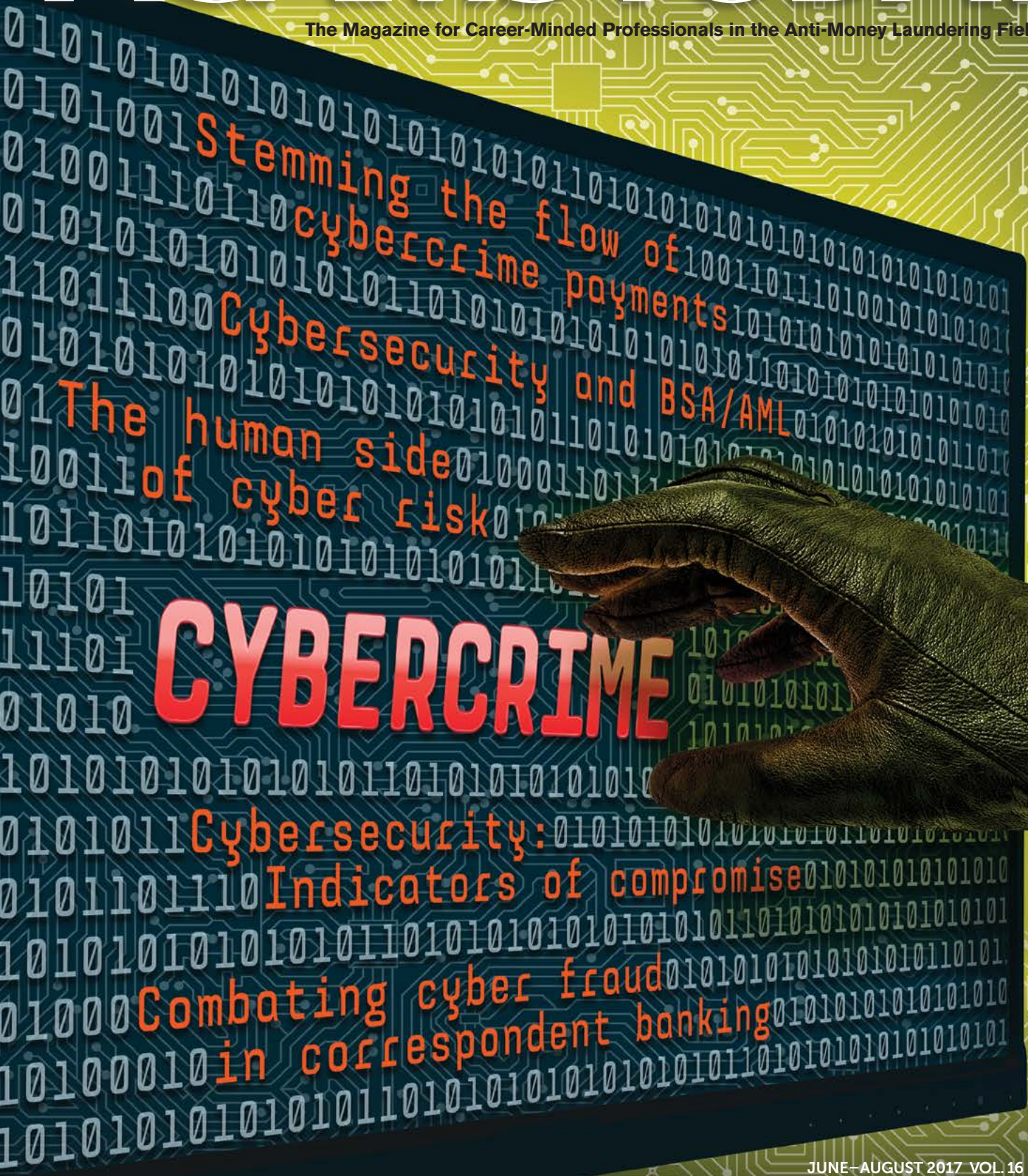


SEVENTH LAW ENFORCEMENT EDITION

ACAMS[®] TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field



CYBERCRIME

Stemming the flow of
cybercrime payments

Cybersecurity and BSA/AML

The human side
of cyber risk

Cybersecurity:
Indicators of compromise

Combating cyber fraud
in correspondent banking

JUNE-AUGUST 2017 VOL. 16 NO. 3

www.ACAMS.org
www.ACAMSToday.org

A publication of the Association
of Certified Anti-Money Laundering
Specialists[®] (ACAMS[®]), Miami, FL, USA

MEASURE, UNDERSTAND & EXPLAIN YOUR MONEY LAUNDERING RISKS

This first-of-its-kind solution helps your institution:

- Identify risks within and across all lines of business
- Mitigate risk by filling in the gaps in your detection and prevention controls
- Present trusted reports that are up-to-par with the latest global regulation and guidance
- Clearly communicate risk to all stakeholders through standardized and automated presentation-ready reports

Schedule a product demo: riskassessment@acams.org



Spiraling compliance costs call for Sustainable Compliance Solutions

We can help you restructure your compliance processes for a more sustainable approach:

- **Optimize compliance operations through program reviews and control enhancements**
- **Overhaul inefficient KYC, EDD and ABC business processes**
- **Manage risk assessment processes efficiently with our auditable, web-based technology**

contact@exiger.com
Exiger.com/compliance-restructured
1 888 990 8424 (US) 0 800 069 8424 (UK)



EXIGER

New York ▪ Hong Kong ▪ London ▪ Silver Spring (DC Metro) ▪ Singapore ▪ Toronto

Governance. Risk. Compliance.

ACAMS[®]TODAY

EXECUTIVE VICE PRESIDENT *John J. Byrne, CAMS*

EDITOR-IN-CHIEF *Karla Monterrosa-Yancey, CAMS*

ACAMS Today, an award-winning magazine, is designed to provide accurate and authoritative information concerning international money laundering controls and related subjects. In publishing this work, neither the authors nor the association are engaged in rendering legal or other professional services. The services of a competent professional should be sought if such assistance is required. *ACAMS Today* is published four times a year for ACAMS members.

To join, contact: ACAMS
Brickell City Tower
80 Southwest 8th Street
Suite 2300
Miami, FL 33130

Tel. 1-866-459-CAMS (2267)
or 1-305-373-0020
Fax 1-305-373-7788
Email: info@acams.org
Websites: www.ACAMS.org
www.ACAMSToday.org

To advertise, contact:
Andrea Winter
Tel. 1-305-373-0020 ext. 3030
Email: awinter@acams.org

| EDITORIAL AND DESIGN |

EDITORIAL ASSISTANT *Alexa Serrano, CAMS*

GRAPHIC DESIGN *Victoria Racine*

| EDITORIAL COMMITTEE |

CHAIR *Debbie Hitzeroth, CAMS-FCI*

Kevin Anderson, CAMS

Brian Arrington, CAMS

Edwin (Ed) Beemer, CAMS-FCI

Robert Goldfinger, CAMS

Jennifer Hanley-Giersch, CAMS

Eric Sohn, CAMS

Joe Soniat, CAMS-FCI

Amy Wotapka, CAMS

Elaine Yancey, CAMS

ACAMS Today © 2017 by the Association of Certified Anti-Money Laundering Specialists (ACAMS). All rights reserved. Reproduction of any material from this issue, in whole or in part, without express written permission of ACAMS is strictly prohibited.

AMERICAN
ADVERTISING
AWARDS



| SENIOR STAFF |

PRESIDENT AND MANAGING DIRECTOR *Tim McClinton*HEAD OF ASIA *Hue Dang, CAMS-Audit*SENIOR DIRECTOR OF OPERATIONS AND CUSTOMER SERVICE *Pierre-Richard Dubuisson*VICE PRESIDENT OF SALES *Geoffrey Fone, CAMS*HEAD OF EUROPE *Angela Salter*

| SALES AND REGIONAL REPRESENTATIVES |

SENIOR VICE PRESIDENT OF BUSINESS DEVELOPMENT *Geoffrey Chunowitz, CAMS*HEAD OF GLOBAL ACCOUNTS *Sonia Leon, CAMS-Audit*HEAD OF AFRICA & THE MIDDLE EAST *Jose Victor Lewis, CAMS*HEAD OF CARIBBEAN *Denise Perez, CAMS*DIRECTOR OF SPONSORSHIP & ADVERTISING DEVELOPMENT *Andrea Winter, CAMS*

| ADVISORY BOARD |

CHAIRMAN *Rick A. Small, CAMS**Luciano J. Astorga, CAMS**Jim Candelmo, CAMS**Robert Curry, CAMS**William J. Fox**María de Lourdes Jiménez, CAMS**Frank Lawrence, CAMS**Dennis M. Lormel, CAMS**William D. Langford, CAMS**Rick McDonell**Karim Rajwani, CAMS**Anna M. Rentschler, CAMS**Anthony Luis Rodriguez, CAMS, CPA**Nancy Saur, CAMS, FICA**Markus E. Schulz**Daniel Soto, CAMS*

| ADVISORY BOARD SPECIAL ADVISORS |

*Samar Baasiri, CAMS**Vasilios P. Chrisos, CAMS**David Clark, CAMS**Susan J. Galli, CAMS**Peter R. Hazlewood*

Contents

From the editor 8

Member spotlights10

A message from the
executive vice president 12

Ending modern slavery:
The financial industry's role.....16

*What the financial industry can do
to identify and disrupt human
trafficking.*



20

The true walking dead:
The apocalypse20

*How financial institutions can
help fight the heroin epidemic.*

Ethically enhanced due
diligence and human
trafficking.....30

*Increased focus on human trafficking
has added to the ongoing narrative
of what is required to satisfy EDD
requirements.*

The success of public-
private partnerships.....46

*How the St. Paul Police Department's
Criminal Proceeds Unit maintains
public-private partnerships.*

Advancing AML programs
while adopting new
technology48

*Six fundamental management
principles needed to meet the
challenges of adopting new
technology.*

The importance of having
a solid compliance culture52

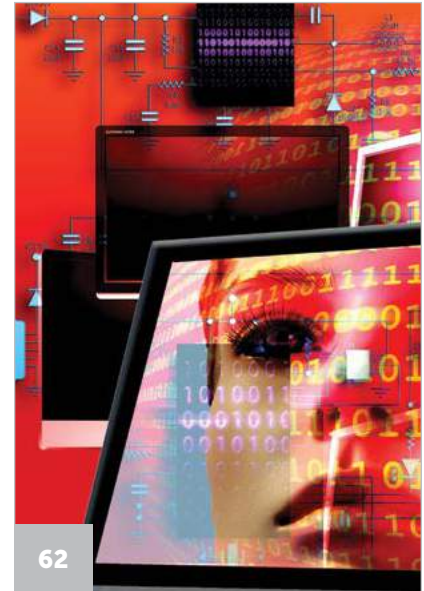
*A culture of compliance can
effectively assist law enforcement
in combating money laundering.*



56

The blocktrain has
left the station.....56

*The risks, trends and solutions
associated with blockchain
technology and cryptocurrency
transfers.*



62

Artificial intelligence:
The implications of false
positives and negatives62

*The differences between false
positives and false negatives and
how they can negatively affect FIs
and law enforcement.*

Islamic terrorism from
a risk perspective64

*Tactical measures to help
thwart terrorist attacks.*

The road to money
laundering centrality.....68

*A look into the evolution
of money laundering.*

Joann Alicea: The fight
against human trafficking/
smuggling continues72

*A discussion of how the public and
private sectors can work together to
help shape the future of SARs for
human trafficking and smuggling.*

ON THE COVER:



The human side of cyber risk ... 14

Identifying potential employees susceptible or vulnerable to committing an illegal act.



Combating cyber fraud in correspondent banking 24

Steps financial institutions can take to protect themselves from cyberattacks.



Stemming the flow of cybercrime payments..... 34

Various ways in which cybercriminals and identity thieves earn money in a cybercrime economy.



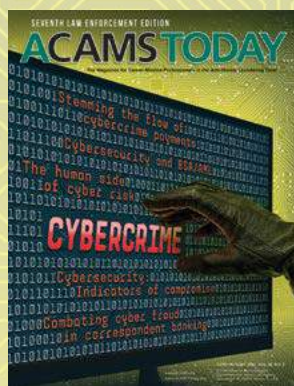
Cybersecurity: Indicators of Compromise 40

Three data points to review in order to be better prepared to file cyber-related SARs.



Cybersecurity and BSA/AML.... 44

Tips for BSA/AML officers venturing into the cybersecurity realm.



IN THIS ISSUE

About this issue:

This edition is dedicated to bringing awareness to cybercrime.

Effectively auditing the four pillars of the screening process 74

How to develop a well-organized periodic auditing system to ensure a strong compliance environment.



From law enforcement to AML and fraud compliance 76

Ways to find meaning after retiring from a law enforcement career.

Interviewing tips for non-IT financial crimes professionals 78

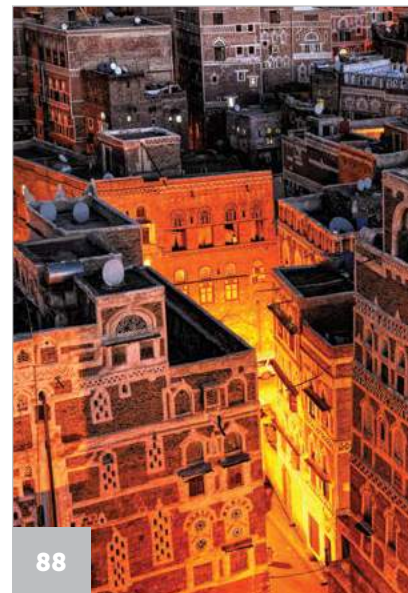
How non-IT financial crimes professionals can prepare for an interview.

White-collar crime: The carousel of VAT abuse 82

The EU's efforts to combat value-added tax abuse.

Dr. Ali Muhsin Ismail: The Iraqi financial system 86

Governor Ali Muhsin Ismail discusses how the Central Bank of Iraq has been improving the Iraqi financial system.



Beyond dedication: AML professionals in Yemen 88

A group of AML professionals take the CAMS exam in Sana'a—a city under siege in Yemen.

Community Banking Corner 92

An introduction to a new ACAMS Today section that will provide useful tips for BSA/AML community bank professionals.

Meet the ACAMS staff..... 93

CAMS and Advanced Certification graduates 94

YOU GOT ~~EMAIL~~ *hacked*

I have a friend who works for the “U.S. State Department” and is equipped with a certain skillset. A few years ago, my friend and I were visiting a mutual acquaintance who was having computer problems. As many of us do nowadays, our mutual acquaintance had his own personal laptop, a family desktop, a work laptop, iPads, etc. Our acquaintance also lived in a typical suburban neighborhood, with the white picket fence and the manicured lawn—well you get the picture.

My friend with the special skillset proceeded to use his own laptop to help our acquaintance with his computer problems. Within minutes my friend (with the special skillset) was asking our acquaintance about different networks, specific folders and even email accounts. My friend had accessed not only our acquaintance's work laptop and his work server, but he also accessed all the information of the entire neighborhood. This was my first experience actually witnessing the rapid speed of hacking that could eventually lead to cybercrime.

Years later, I had another friend whose company had been a victim of email spoofing. The interesting part of cybercrime is that it does not discriminate—any person, or race of any socio or economic class can be duped.

The Seventh ACAMS Today Law Enforcement edition is dedicated to bringing awareness to cybercrime and the different ways this security breach touches everyone, everywhere and at any time.

The human side of cyber risk identifies potential employees who could be susceptible to committing cybercrime and how they might be a financial institution's greatest risk.

Combating cyber fraud in correspondent banking describes how cybercriminals have changed their focus on attacking banks directly and what steps you can take to secure your financial institution.


Stemming the flow of cybercrime payments discusses the international nature of cybercrime and how cybercriminals monetize their gains and move their funds.

In addition to more cyber-related articles, the *Seventh Law Enforcement* edition contains articles on human trafficking prevention, partnerships between the financial sector and law enforcement, blockchain technology and cryptocurrencies, career guidance for those leaving the public sector and moving into the private sector and interviewing tips for landing your next job.



The MENA Report section contains an inspiring article about the dedication of our members in Yemen in the midst of a war-torn country.

Furthermore, we are also introducing a new section to the *ACAMS Today* publication: *The Community Banking Corner*. *The Community Banking Corner* will contain tips for community bankers and focus on all Bank Secrecy Act/anti-money laundering aspects.

I would like to thank our law enforcement members for their dedication and commitment in the fight against financial crimes. Finally, I would like to encourage everyone to be more vigilant so that we do not become victims of cybercrime. 

Karla Monterrosa-Yancey

Karla Monterrosa-Yancey, CAMS
editor-in-chief

SARSTRIPS™



Produced by: ComplianceComm



Know the unknowns.

Thomson Reuters delivers trusted answers for KYC due diligence.

Go deeper in your investigations and reveal connections other resources miss. With Thomson Reuters World-Check® and CLEAR®, you retrieve faster, more relevant results to help you find the answers. It's the easy way to uncover people, assets, businesses, affiliations, and locations.

And with integrated reports, you can easily share your findings.

Take your KYC further with World-Check and CLEAR.

legalsolutions.com/kyc-solutions

The intelligence, technology and human expertise
you need to find trusted answers.



the answer company™

THOMSON REUTERS®



**Allan Clare, CAMS, FCII, FCILA, CFE, Dip (Fin.Crime), MICA
Birmingham, U.K.**

Allan Clare has held a number of anti-fraud, financial crime compliance and risk management leadership roles with the U.K. and global financial institutions. Clare is currently the head of financial crime compliance at HSBC U.K., the newly created ring-fenced bank, formed to comply with the U.K.'s Banking Reform Act. Clare, who sits on the HSBC U.K. Executive Committee, is responsible for the financial crime risk management program, including anti-money laundering (AML), sanctions and anti-bribery and corruption across all lines of business.

In addition, he is a Certified Anti-Money Laundering Specialist, Certified Fraud Examiner, Member of the International Compliance Association with whom he holds a Diploma in Financial Crime, Chartered Insurer and Fellow of the Chartered Insurance Institute, Chartered Loss Adjuster and Fellow of the Chartered Institute of Loss Adjusters where he was instrumental in forming the Institute's Fraud Special Interest Group and was its inaugural chairman.

Clare is actively involved in numerous U.K. financial services industry and trade body groups and is a member of the management board of the Joint Money Laundering Intelligence Task Force. Previous roles include chairman of the Financial Intelligence Unit Working Party at the Wolfsberg Group, board director of the Insurance Fraud Bureau, director of CIFAS, deputy chairman of the Insurance Fraud Investigators Group and member of the Association of British Insurers Financial Crime Committee, where amongst other responsibilities he led the project that created the industry-funded City of London Police Insurance Fraud Enforcement Department.



**Scott DeRycke, MBA, CAMS
Mahomet, IL**

Born and raised on a family farm in Central Illinois, Scott DeRycke graduated from Illinois State University in 2006 with a degree in criminal justice. In 2012, he graduated from Utica College with an MBA in economic crime and fraud management. He received his CAMS certification in 2014. He has over six years of experience in mortgage compliance, mortgage due diligence, mortgage servicing, enhanced due diligence and anti-money laundering compliance with banks and consulting firms.

DeRycke is currently working as a consultant for Mission Capital Advisors, a mortgage due diligence firm. Mission Capital Advisors works on due diligence projects for several small and large banks. As a consultant, DeRycke is responsible for compliance file reviews, collateral file auditing and due diligence reviews. In addition, he has been a member of ACAMS since 2012 and has attended several webinars, seminars and conferences as a member.



**Did you know that
ACAMS' new Cyber-
Enabled Crime
Certificate course
begins in June?**




**Christine Miller, CAMS
Millbury, MA, USA**

Christine Miller's banking career spans over 30 years. She has always been passionate about compliance and has worked independently to develop her knowledge and skills in the compliance field. As a compliance officer at her previous company, she utilized her passion and compliance knowledge to develop the institution's compliance policies and procedures and train employees.

In 2015, she became the Bank Secrecy Act/anti-money laundering (AML) officer at Millbury Federal Credit Union and in 2017, she was appointed as the security officer. As part of her goals to continue increasing and enhancing her compliance knowledge, she studied for and obtained her CAMS certification in 2016. According to Miller, the knowledge that she attained through the CAMS program has helped prepare her for the investigations that she performs in her current role. In addition, she is a member of the Eastern Mass Compliance Network and Worcester County Risk Management.

As a security officer, Miller is responsible for all AML and counter-terrorist financing investigations and all OFAC responsibilities for the credit union. She reports all pertinent information for review to the board of directors.

As an active member of her community, Miller has volunteered at financial literacy outreach programs for a variety of local groups and she volunteered at veteran associations, Girls Choice, ESL programs and other community organizations. In addition, as security officer, she is developing a program to reach out to senior citizens to better educate them on how to protect themselves against the different scams that are targeting the elderly. **A**



Reduce fraud. Mitigate risk.
Improve productivity. And
lessen customer friction.



LexisNexis® Risk Solutions offers market-leading solutions across the onboarding, screening and due diligence workflow. With unparalleled data assets and proven analytic and linking technology, we can help with:

ID Document Checks: Available in over 200 countries, automatically check that a customer's ID document is valid.

Identity Verification: Screen and verify customer identities by accessing a database with billions of records from 32 countries.

Anti-Money Laundering: Mitigate risk through comprehensive sanctions, enforcement, watchlist and PEP screenings.

Adverse Media: Reduce reputational risk by accessing a media database with thousands of newspapers and trade journals.

For more information, call, email or visit us online:

Singapore: 800 120 6351
China: 400 120 2848
Hong Kong: 800 964 868
Malaysia: 1800 817 621

solutionsinquiry@lexisnexis.com
lexisnexis.com/risk/apac

CONTINUING OUR TRIBUTE TO **LAW ENFORCEMENT** WITH NO ALTERNATIVE FACTS

In writing this article for the seventh law enforcement edition of *ACAMS Today* and recognizing the many successes of law enforcement, I am struck by the missed opportunities for anti-money laundering (AML) professionals to communicate how important that group is to fighting financial crime. I also wonder if true law enforcement “supporters” actually listen to themselves.

For example, ACAMS is fortunate to have a number of members who work or have worked for the Internal Revenue Service (IRS). IRS investigators deal with a wide array of issues such as money laundering, identity theft, cyber and of course, tax evasion. They are a respected agency by our community, but politicians will try to benefit by attacking the mission of the IRS and then pretend they support law enforcement—you cannot have it both ways.

This edition focuses intensely on the global problem of cyber-related crimes and security issues. Policymakers of all stripes will bemoan the danger of attacks on the internet, but then some will support allowing broadband providers in their efforts to roll back “net neutrality” and permit more use of personal information.

The area of human trafficking also continues to harm our society and needs public-private partnerships to continue

to thrive and combat this global outrage. We have been very vocal about the excellent work of government agencies such as the Department of Homeland Security (DHS) in the U.S. and FINTRAC and law enforcement in Canada (Project Protect). All of those entities would also admit to the need for private sector partnerships and those are happening. What frustrates those of us that follow this problem is a diversion of resources toward arresting and deporting non-criminals instead of those that prey on trafficking victims. Again, you cannot have it both ways.

In our Washington, D.C. chapter, we had a compelling presentation and dialogue on the opioid epidemic that harms people of all ages. Led by ACAMS award winner and frequent *ACAMS Today* author Jim Cox, those in attendance not only learned about the severely addictive nature of opioids and the potential “red flag” financial indicators, but also about how best to raise awareness on this societal scourge. What is missing, however, is supporting law enforcement by getting the medical community to stop prescribing unusually high doses for prescriptions and to call policymakers to task for cutting funding for needed programs.

Finally, ACAMS has spent a great deal of time in the past year working on the infamous “de-risking” (financial access) issue and I have to point out that we were the first to emphasize the impact on law enforcement when financial institutions exit or fail to onboard certain entities because of risk. It is clear that some financial institutions have a greater risk appetite and mitigation protocols than others, so the loss of oversight, whether due to regulatory confusion or revenue loss, can harm law enforcement’s access to data, financial intelligence and suspicious activity reports.



Law enforcement must be at the policy “table” while we tackle this problem, but others frequently forget that.

Cyber—Our greatest challenge?

This is our first law enforcement edition dedicated significantly to one subject. Cyber-enabled crime and cybersecurity encompass so much in 2017 and demands our collective attention. In this edition, you will see articles dedicated to government guidance, electronic banking vulnerabilities and the potential misuse of law enforcement information for nefarious purposes.

We would also point out that ACAMS is posting a “Cyber Resource” page and we would love your feedback and comments.

A tribute to a retiring public servant

By the time we publish, IRS-CI Chief Rich Weber will have left that agency. He will still give us the benefit of his expertise in a new role in the private sector, but we would be remiss if we did not thank Rich for his public service and work with financial institutions on a number of critical issues.

Thanks, Rich! We look forward to your next endeavors in assisting the AML community. 

A handwritten signature in black ink, reading “John J. Byrne”.

John J. Byrne, Esq., CAMS
executive vice president



■ Spot the dirty money. Stay compliant.

If money laundering were an economy, it would be the fifth largest in the world.

We have to unite against this underground economy.

It's time for industry, government, technology and compliance specialists to join forces and tackle money laundering.

It's not just security. It's defense.

Learn more at BAESystems.com/financialcrime

BAE SYSTEMS

THE HUMAN SIDE OF CYBER RISK

Spend time with retired four-star General James Jones and you will likely hear his ominous bifurcation of “those companies that have been a target of a cyberattack, and those that will be.” As former U.S. National Security Advisor to the President and Commandant of the Marine Corps, General Jones dedicated his career to understanding, mitigating and preventing security risk at all levels.

Commercial industry has been actively addressing cyber risk for decades while attacks have only increased in frequency and severity. Most people associate cybercrime with external threats and nation states and criminal hacking into a company's network. A lot of investment has been dedicated toward protecting the perimeter and keeping these bad actors out. The reality is that cybercrime is committed by a combination of individuals outside and inside a company. Insiders, those who the company either recruited or hired, often account for half the financial loss and crime.

Criminal theory tells us that crime is a function of motivation and opportunity. To address the rising concern of insider threat, most organizations have almost entirely focused their efforts on the opportunity side of this equation: monitoring digital activity within the workplace and controlling access to limit opportunity. This form of internal network monitoring may include access and movement of files, folders, documents, websites, as well as internal email communication. The objective is to identify, understand and document suspicious, illicit or illegal activity and then limit or shut down access to sensitive, confidential or financial data.

Think of this as the final line of defense. The threat has become active. The crime is being attempted now. The plan is to identify the initial activity fast enough to remove or negate the opportunity and protect the organization from a crime in progress.

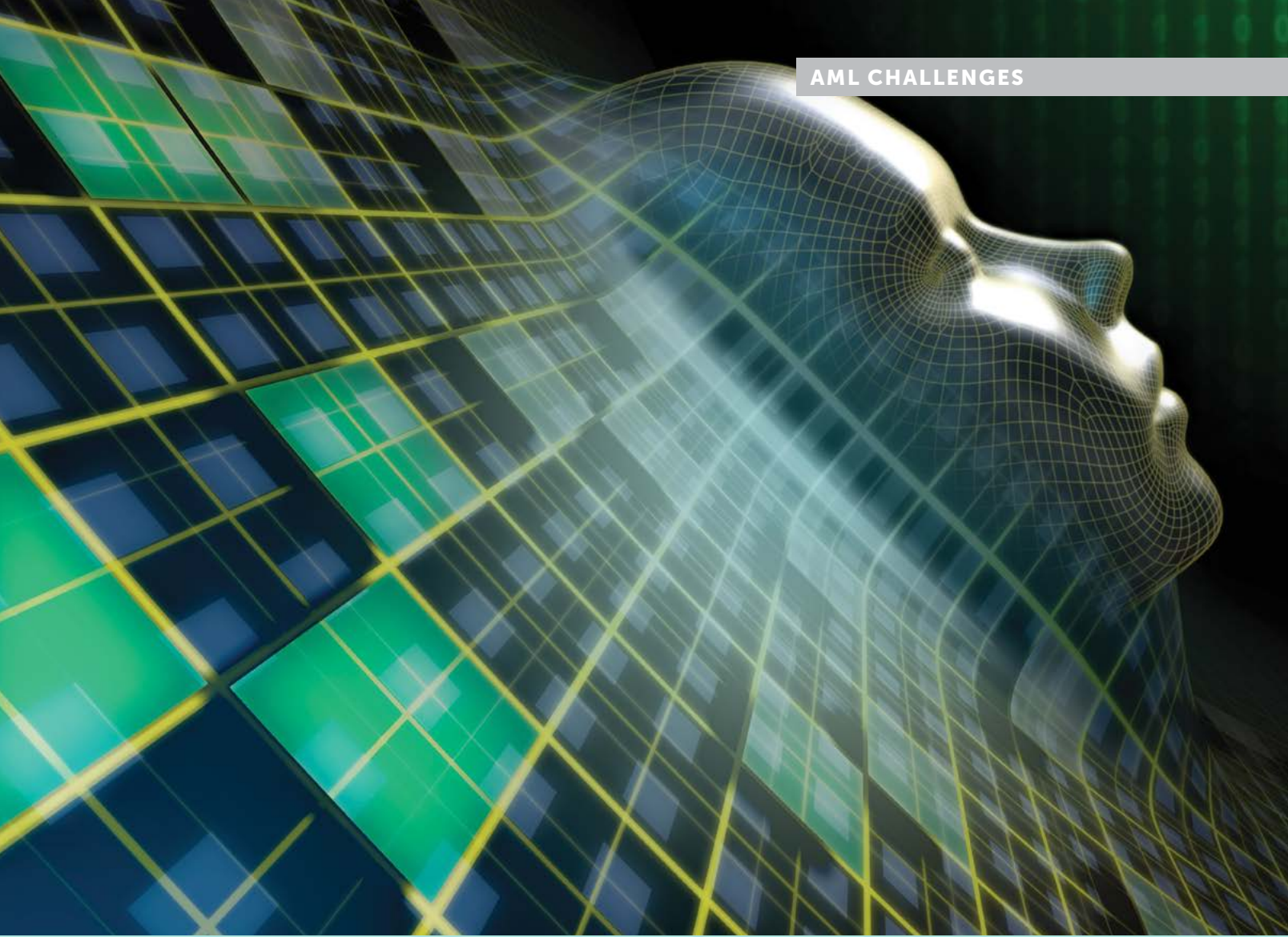
Today, companies not only defend against cybercrime but aim to stop emerging threats posed by the insider by expanding their focus to the human side of this risk. Most cyber experts agree that people (employees) are usually the most vulnerable link in a company's cyber defense. Many organizations view this employee risk through the lens of careless keystrokes or poor cyber hygiene (“do not click that link,” “do not open that document,” “do not use the word ‘password’ as your password”). This human risk is a function of undereducated or inadvertent behavior. Risk caused by negligent behavior can be addressed through proper training and procedure.

Unfortunately, not all human risk is driven by error. Insiders can also consciously engage in illegal activity, so companies must understand and address the motivational aspects of crime. Consider that employees do not just suddenly show up for work one day and decide to defraud their company or commit an act of cybercrime. Certain specific events and circumstances pre-date workforce crime.

The key for companies is to identify those employees that are susceptible to commit an illegal act or vulnerable to the influence of nefarious external actors looking to exploit them for financial gain. These are employees who, unbeknownst to their company, are under criminal, financial or other personal stress. These individuals are the hardest of threats for an organization to defend against. Because of their insider status they can understand and learn the company's defense systems and work to bypass or suppress them.

For the good of the employee, coworkers and the organization, companies must always be aware of material changes to employee behavior both in and outside of the workplace. Know your employee initiatives emphasize the need to seek a holistic picture of your employees over time, as well as the timely identification of aberrations or unusual patterns of high-risk behavior (for example, repeat or escalating criminal activity outside the workplace or sudden and drastic changes to someone's personal financial condition). Such behavior, which would have been disqualifying in the hiring process, may occur six months, a year or five years later and remain undetected, thus adjudicated by the organization.


People's lives change all the time for common reasons (e.g., they get married, have children, buy and change homes, care for family members, pay for college and/or cope with medical challenges). Significant change can produce a level of personal stress that often is temporary or addressed through constructive and positive behavior. However, sometimes high levels of stress can spiral out of control, and many times it is not obvious to family, friends, coworkers and managers.



The human side of cyber risk management is inherently people-oriented. The key to any organization is finding the balance between the risk management goal of protecting an organization and the personnel goal of building a culture of trust. The answer is not to accumulate as much employee data as possible (i.e., sifting through good and bad behavior hoping to identify risk). In addition, it is not about continually rerunning background checks or monitoring the everyday, common behavior of your employee base when they leave the office.

The solution must be event-based, seen in real time, actionable and driven by those specific behaviors your organization deems high-risk within the context of your industry, your company, and each employee's role. For example, a company would almost certainly define a financial controller being arrested for check fraud or an employee who drives a company car being arrested for DUI as high-risk behavior. Certain roles are indeed mission critical and timely alerting is essential to risk mitigation. Contextual policy is important because not every employee has the same level of access to financial transactions, customer personally identifiable information, credit card accounts or sensitive data.

The solution must also support the rights and privacy of employees. Technology can help standardize execution, ensure legal and regulatory compliance, drive proactive and transparent cyber risk policy and most importantly remove personal bias and ad-hoc judgmental decision-making. That is how you strike a balance in protecting both the organization and the individual for success.

Finally, insider risk management is not limited to solely protecting the organization from cybercrime. With early leading indicators and warning signs of behavioral risk, companies can now assist employees who are not asking but need help. The company can intervene at a time where behavior can be positively modified through training, counseling or one-on-one interaction. Course correcting behavior can better ensure an employee's success in a current role and a long-term career path. The ultimate win is realized when companies prevent insider risk from occurring well before it places an employee's job at risk or becomes an actual insider threat to the organization. 

Tom Miller, CEO, ClearForce, Vienna, VA, USA, tmiller@clearforce.com

ENDING MODERN SLAVERY:

The financial industry's role

Human trafficking—a form of modern slavery—is one of the fastest growing criminal activities in the world. It exploits an estimated 45 million people a year¹ and generates approximately \$150 billion in profits.² Though the concept of human slavery is certainly not new, some are unaware of the impact and extent of human trafficking in the 21st century, both at home and abroad.

The good news is that the financial industry can play a part in disrupting this heinous crime. With proper education, knowledge of red flags and victim indicators, and by building strong relationships with law enforcement, the financial industry can help disrupt the problem of modern slavery.

Hidden in plain sight

According to the Foundation for a Slavery Free World,³ there are 20 to 30 million slaves in the world today. The Global Slavery Index⁴ estimates upwards of 40 million. In the U.S., the statistics are equally jarring. The National Coalition Against Domestic Violence reported that approximately 80 percent of trafficking involves sexual exploitation and 19 percent involves labor exploitation.⁵ According to the U.S. State Department, 600,000 to 800,000 people are trafficked

across international borders every year, of which 80 percent are female and half are children.⁶

The Action Means Purpose (A-M-P) model⁷ on page 19 is helpful in understanding the definition of human trafficking. Yet the extent of the problem remains a bit more difficult to define. “Hidden in plain sight” is a term used in the Department of Homeland Security’s Blue Campaign, an effort that aims to combat human trafficking. This phrase represents the difficulty of spotting human trafficking on the surface.

In a 2015 edition of *Frontline*, the Public Broadcasting Service illustrated the divergence between reported instances of human trafficking and actual arrests in the U.S.⁸ The article noted that in 2014, a federally funded hotline for U.S. trafficking victims received more than 21,000 calls. During that same period, the Department of Justice made only

184 convictions for trafficking, which shows the disparity between reports and arrests.⁹

As former Secretary of State John Kerry said in the *2015 Trafficking In Persons Report*, “Whether we are talking about the sale of women and children by terrorists in the Middle East, the sex trafficking of girls lured from their homes in Central Europe, the exploitation of farm workers in North America, or the enslavement of fishermen in Southeast Asia, the victims of this crime each have a name.”¹⁰

Each victim has a name

Tenancingo, Mexico is widely considered the sex trafficking capital of the world. It is the single largest source of sex slaves to the U.S.¹¹ Men who are masters of manipulation kidnap boys and girls as young as 14 years old from Tenancingo’s surrounding villages. They trick, threaten or seduce them into working for the sex trade. Many times these pimps capitalize on the residents’ values by pretending to start a relationship with them, telling them they love them and tricking them into a life of slavery.

Ultimately, the victims find out that they have been lured away from home in a prostitution or labor scheme, getting paid very little for very poor working conditions against their will. “He said the money was to buy land so we could build a little house, but it was all false, even the name he’d given me was false. He made me live a very sad, ugly, desperate life,” one victim told *The Guardian* in 2015.¹²

¹ The Global Slavery Index, 2017, <http://www.globallslaveryindex.org/findings/>

² International Labour Organization, 2014, <http://www.ilo.org/global/topics/forced-labour/lang--en/index.htm>

³ Foundation for a Slavery Free World, 2015, <https://www.slaveryfreeworld.org/>

⁴ The Global Slavery Index, 2017, <http://www.globallslaveryindex.org/findings/>

⁵ The CNN Freedom Project, *CNN*, October 18, 2013, <http://thecnnfreedomproject.blogs.cnn.com/category/the-facts/the-number/>

⁶ Trafficking In Persons Report, United States Department, 2004, <https://www.state.gov/documents/organization/34158.pdf>

⁷ National Human Trafficking Resource Center (NHTRC), 2017, <https://humantraffickinghotline.org/resources/actions-means-purpose-amp-model>

⁸ Caroline Reilly, “Human Trafficking: A Crime Hard to Track Proves Harder to Fight,” *Frontline*, July 29, 2015, <http://www.pbs.org/wgbh/frontline/article/what-is-human-trafficking-and-why-is-it-so-hard-to-combat/>

⁹ “Trafficking In Persons Report,” U.S. Department of State, July 2015, <https://www.state.gov/documents/organization/245365.pdf>

¹⁰ Ibid.

¹¹ Natasha Bertrand, “This Mexican Town is the Sex Trafficking Capital of the World,” *Business Insider*, February 10, 2015, <http://www.businessinsider.com/this-mexican-town-is-the-sex-trafficking-capital-of-the-world-2015-2>

¹² Nina Lakhani, “Tenancingo: The Small Town at the Dark Heart of Mexico’s Sex-Slave Trade,” *The Guardian*, April 4, 2015, <https://www.theguardian.com/world/2015/apr/05/tenancingo-mexico-sex-slave-trade-america>

However, trafficking is not just contained to communities like these. The problem is happening in our own backyards and even in wealthy neighborhoods and non-border states. Human trafficking affects people of all genders, ages and nationalities — even domestically.

A close-to-home example is Backpage.com. Backpage is the world's largest classified ad company. According to Dawn Hawkins, executive director of the National Center on Sexual Exploitation, Backpage posts 1 million prostitution ads a day.¹³ Earlier this year, a Senate subcommittee published a report, after a 21-month investigation, finding that Backpage knowingly facilitated online child sex trafficking on the “adult” section of its website.¹⁴ Many of the girls advertised were victims of trafficking. The adult section was taken down, but according to *CNN*, sex advertisements began to appear on a different section of the website.¹⁵

The first step in being able to identify and disrupt human trafficking—from a financial institution's perspective—is awareness

“It’s not just a border issue,” said Harry Jimenez, deputy chief of Bexar County Sheriff’s Office in San Antonio. “More and more human trafficking victims are found in the interior of the United States. They are trafficked through the major highways of the United States, and the traffickers are looking for smaller communities with smaller banking communities,” said Jimenez. “They believe the bankers have fewer resources than a big

bank would, and they know that the law enforcement is more limited and they’re not going to be conducting sting operations, for example,” said Jimenez. These examples illustrate that sex trafficking and labor trafficking are happening in the U.S., in large cities and in small towns, and even in our own backyards.

How can the financial industry make an impact?

Law enforcement is not the only group that is challenged by the “hidden in plain sight” problem. The financial industry can often find it difficult to identify signs of human trafficking. The money is moved quickly and quietly, and the transactions may not always appear suspicious on the surface. However, anti-money laundering (AML) professionals can make an impact to identify and prevent human trafficking if they are armed with the proper knowledge.

The first step in being able to identify and disrupt human trafficking—from a financial institution's perspective—is awareness. It is important not only for compliance professionals to be educated and keep up-to-date with the issue, but also to train other staff on it. AML professionals can incorporate information about human trafficking into their required training—what it is, red flags to look for on the front end and more.

Counter-human trafficking activities should also be built into an institution's customer due diligence policies and procedures. Asking the right questions, knowing what to look for, and thinking holistically about known patterns and indicators of human trafficking all play a part in customer due diligence. Bank Secrecy Act/anti-money laundering software automation can also be a significant factor in the ability to flag potentially suspicious transactions based on rules, behaviors and/or typologies related to human trafficking.

Financial red flags for human trafficking

There are hundreds of red flags that may indicate human trafficking, from victim indicators to transaction traits. Sometimes this requires thinking outside the box, beyond just the cash intensive businesses. Jimenez used business customers in the service industry as an example. “It goes back to know your customer,” he said. For example, in doing due diligence on how many employees a company has, AML staff would look at whether the business has a payroll account. “You’d be surprised how many massage parlors and nail salons that are being involved in sexual exploitation don’t have a payroll account, because nobody’s getting paid,” he said.

In addition, there are certain victim indicators of trafficking, which can indicate coercion, brainwashing and so on. For instance, a trafficking victim may be accompanied by a controlling person or boss and will not speak on his or her own behalf. Individuals may have a lack of control over their personal schedule, money, ID or travel documents. They may be transported to or from work, or living and working in the same place. “Many of these victims of sexual exploitation and human trafficking... [are] unable to identify themselves as victims,” said Jimenez. “These individuals are unable to go to a police officer and say, ‘I need help.’”

Customers’ profiles can also contain red flags. Customers with excessive numbers of accounts, consumers with discrepancies between account funding and known customer profile, and businesses or industries easily exploitable by traffickers (immigration attorneys or labor intermediaries) can all require further investigation.

¹³ Dawn Hawkins, “Statement: Backpage.com Block Prostitution Ads in U.S. Under Pressure for Sex Trafficking,” National Center on Sexual Exploitation, January 10, 2017, National Center on Sexual Exploitation. <http://endsexualexploitation.org/articles/statement-backpage-com-blocks-prostitution-ads-u-s-pressure-sex-trafficking/>

¹⁴ Ibid.

¹⁵ Andrea Powell, “The Fight Against Sex Trafficking is Bigger than Backpage,” *CNN*, January 19, 2017, <http://www.cnn.com/2017/01/18/opinions/backpage-sex-trafficking/>

There are also several transaction traits that can be red flags, many of which are detectable using a suspicious activity detection engine. One example is a high volume of round-dollar deposits via wires, ACH, or cash in the range of \$2,000 to \$3,000, which could indicate payment to the trafficker. The person is moved to a large city like New York, for example. The money is transferred to the trafficker in another location, possibly a border town. The dollar amounts are low, as a human commodity continues to generate profits.

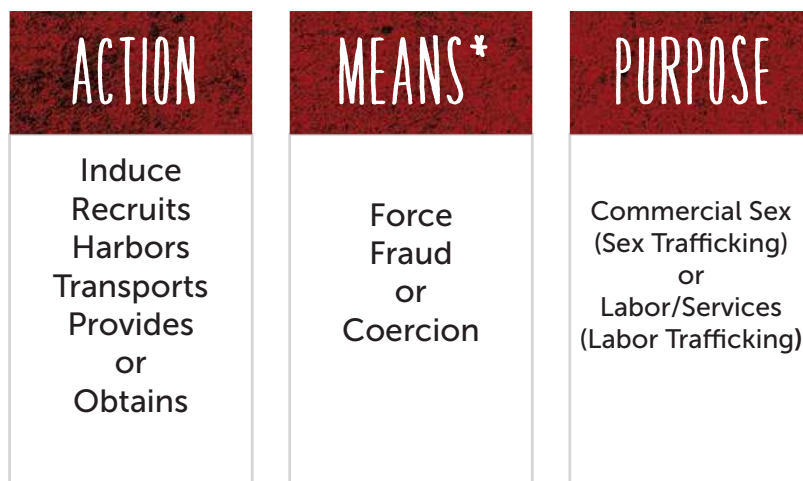
Other indicators include excessive interstate or intrastate cash deposits less than \$1,000 at multiple branches daily, as well as cash deposits just below the currency transaction reporting threshold but deposited at several branches. A high volume of debit or credit card transactions using specific merchant codes, airline/rental car/bus/taxi charges in multiple cities and states, and excessive hotel charges with high percentages or purchases made at high-end merchants and casinos, can also be red flags. Extensive payments to web advertisers that cater to the sex industry, extensive purchases of money orders to pay bills, wire transfer activity inconsistent with the customer's business, and wires to or from origin or staging countries that are inconsistent with the customer's known profile can be indicators as well, just to name a few.

The problem with human trafficking may never be visible in plain sight. However, there are certain indicators for which AML professionals can monitor. When red flags are identified or suspected, the next step is reporting it.

Working with law enforcement to bridge the gap

AML professionals know the importance of working with law enforcement to prevent financial crime, and this is particularly relevant to counter-human trafficking efforts. Strong partnerships and relationships with law enforcement, nongovernmental organizations, consortiums and anti-trafficking coalitions can be critical in disrupting the issue.

THE A-M-P MODEL



* Minors induced into commercial sex are human trafficking victims—regardless if force, fraud or coercion is present.

Source: National Human Trafficking Resource Center (NHTRC), 2017.
<https://humantraffickinghotline.org/resources/actions-means-purpose-amp-model>

“What we recommend as law enforcement,” said Jimenez, “is to develop this relationship with your law enforcement community. State and local law enforcement will have someone working in human trafficking or organized crime. Look for those individuals.”

On the federal side, Homeland Security Investigations is a resource. “There will be a Homeland Security Investigations close to you,” said Jimenez. He pointed out that Homeland Security offers free training. They will provide the latest red flags for communities and financial institutions. “These are the same individuals that will come and respond to your SARs,” he said.

When in doubt, file the suspicious activity report (SAR). Even if it is just a suspicion that human trafficking may be present, include the following in the SAR narrative: “It appears like possible human trafficking.” Trust your gut instinct as a professional. If it looks suspicious, it probably is. “You may not know it’s human trafficking, but the fact that you’re writing the SAR is the first step,” said Jimenez.

Human trafficking is a billion dollar industry and it is impacting the entire globe. Even in the U.S. people are being sold as sex and labor slaves, confined to working in illegal and dangerous conditions against their will. Many of them are children, and many of them will die in servitude. However, financial institutions have the power to identify, prevent and disrupt human trafficking activity. As a society, we still have a long way to go. Yet as AML professionals, our work truly makes a difference in bringing justice to victims and ending modern slavery for good. 🇺🇸

Terri Luttrell, CAMS-Audit, manager of professional services, Banker's Toolbox, Austin, TX, USA, terril@bankerstoolbox.com

Emily Gasper, marketing content specialist, Banker's Toolbox, Austin, TX, USA, emily.gasper@bankerstoolbox.com

The true walking dead: THE APOCALYPSE

As written in the 2016 *ACAMS Today* law enforcement edition, this article is not meant to embarrass, put down, or offend persons suffering from addiction. However, it is a wakeup call to the readers of this article, to us as a society, and to the world we share.

In 2015, 52,404 people died from an overdose in the U.S. Brothers, sisters, aunts, uncles, mothers, fathers, and our own children abused legitimate and illegitimate drugs, suffered an overdose and died. This is not just a U.S. problem, search the internet and look at the numbers in your country.

As 2016 numbers are totaled across the county here in Virginia, 1,420 died from an accidental overdose, once again this number surpassed motor vehicle and gun-related deaths. These numbers can rise as bodies lay in morgues awaiting lab results to the cause of death.

SYNTHETICS FLOOD THE MARKET

Fentanyl, created in 1960, is a synthetic opioid and reported to be 50 to 100 times more powerful than morphine. It can also be 10,000 times more potent than morphine, depending on production. In 2016, the U.S. began to see heroin cut with fentanyl and at times pure fentanyl was being sold by illicit dealers. Fentanyl

does have legitimate use—it treats chronic pain. However, like other legally prescribed drugs such as oxycodone and oxycontin, it is abused by persons looking to get high. In addition, fentanyl is being disguised in different pill forms. It will look like a pill of a different drug, but it is in fact pure fentanyl.

Carfentanil is another synthetic opioid created in 1974 and is reported to be 10,000 times more potent than morphine. It is mostly used as a general anesthetic for large animals like elephants. In the 2000s, Eastern Europe saw a surge of illicit use by persons and in 2016, the U.S. began to see it being abused by users searching for that ultimate high. The use and abuse by humans across the globe have led to numerous deaths.

Local dealers who either cut it with heroin or sell it in its pure form sell both of these drugs. States across the U.S. are reporting more and more overdose deaths from both of these drugs. States are also seeing illicit dealers selling a street named drug called “Gray death.” It is a combination of heroin, fentanyl, carfentanil, and a synthetic opioid branded U-47700, also known as “Pink” on the street. Users do not care what is in the dose they are taking as long as it gets them high.

Last year in Fairfax County there was a house party hosting young adults and juveniles. The attendees, mostly high schoolers, enjoyed each other's company, listened to music and danced. A young man sold morphine during the party. The next day a 17-year-old girl was found dead. She overdosed on the morphine she purchased. The young man was tried and convicted and is now serving eight years in prison.

WHY THIS ARTICLE IS TITLED THE TRUE WALKING DEAD: THE APOCALYPSE

As a local law enforcement agency, we cannot go anywhere we want and enforce drug laws. With that said, we just pick up the telephone and contact a local or federal partner. We are currently working on a case where a person is buying heroin for us to build a case on a dealer supplying our county. A detective went to a local city not far from Fairfax County with a federal partner. While sitting on a street waiting for the deal to take place, the detective described seeing at least 20 people walking down the sidewalk at different times as if in a zombie-like state. If you have ever seen anyone on heroin, you will understand the meaning behind the title.

DRUGS ARE NOT A VICTIMLESS CRIME

If you think that this epidemic does not affect you because you do not know anyone suffering from addiction, think again. Society's lack of education on this crisis places people in harm's way.

Case one

A car is dropped off at a tire repair shop for four new tire replacements. The technician goes into the glove compartment to look for the locking lug key. As he searches, he feels a sharp pain immediately in his finger. He realizes he is being pricked by an uncapped and used syringe. The car owner is a daily heroin user. The technician must now go through a battery of medical tests and

will constantly have to worry if he will contract a variety of diseases common with heroin users.

Case two

A dental assistant is at the office meeting with patients cleaning teeth and providing dental aid to the dentist. In between patients the assistant enters the office restroom, uses heroin laced with fentanyl, overdoses and dies. The fire department is called as they cannot get into the bathroom. The door is removed and the assistant is found. This can easily be the dentist you have been going to for years.

Case three

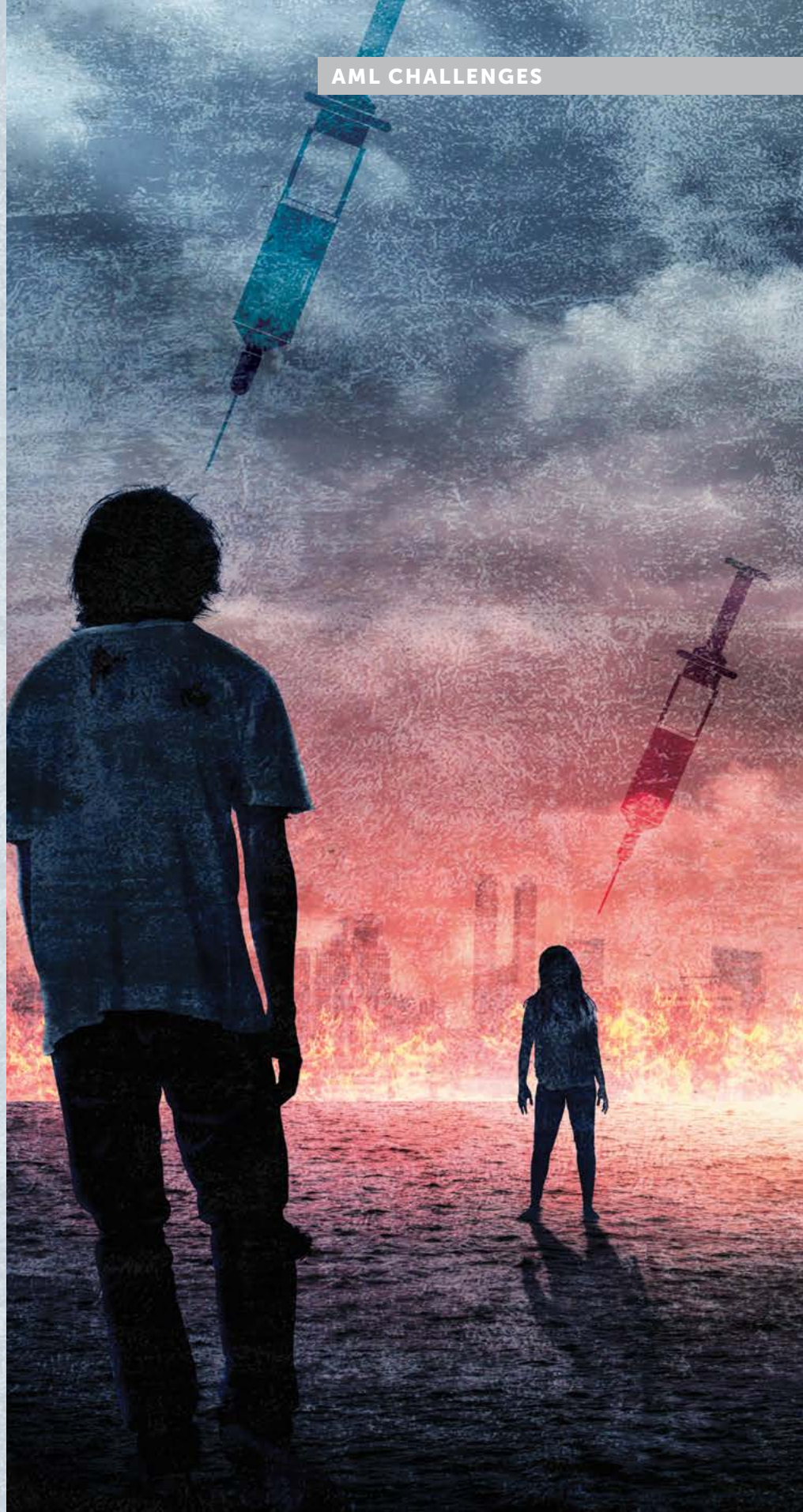
You are shopping with your family at your local grocery store. Unbeknownst to you, a young woman is in the restroom shooting up heroin. Her boyfriend tries calling her to see what is keeping her and cannot reach her. He finds her in the restroom unconscious and overdosing. Instead of calling 9-1-1, he drags her unconscious body (still with a syringe in her arm) through the store in front of your family, in hopes of not being arrested.

Case four

A husband and wife go to their local drug dealer and purchase heroin. They drive to a park where children are playing soccer. It is a nice day, so the couple open the car doors and the husband is the first to inject himself with the heroin purchased. He immediately overdoses and falls partially out of the car. The wife thinks to herself, "Wow that must be good heroin," so she pulls out the needle from her husband's arm and injects herself with the remaining dose. She begins to overdose and falls partially out of the car unconscious. It is first reported to 9-1-1 as a double homicide. It is later determined to be a heroin overdose. This occurred in front of kids playing soccer.

Unfortunately, these are true stories and there are thousands like them. This epidemic is happening all around us. The picture on page 22 was put on the internet by the East Liverpool Police Department. Notice the child in the back seat.

This vehicle was being driven and was stopped by police for erratic driving behavior. The vehicle was directly behind a school bus carrying children. The driver was charged and pled guilty in his court proceeding. The grandmother in the passenger seat was charged as well





and is awaiting her trial. The child was placed with county child services. This all occurred in front of the gazing eyes of children onboard a school bus. Do you still think there are no victims?

EDUCATION

In the article I wrote in the June-August *ACAMS Today* 2016 edition I discussed and asked the readers to view the film *Chasing the Dragon: The Life of an Opiate Addict*. Just recently, the ACAMS U.S. Capital and Virginia Chapters held a joint event to discuss this continuing epidemic. I was amazed when I asked the crowd of more than 70 if they have seen the film—only a handful raised their hand. The event started with the showing of the film. The film was eye opening to some. Someone in the audience shared that they live with a family member who suffers from addiction. Others were shocked to see ordinary people going through the horrors opioid addiction creates.

I am a firm believer that knowledge is power and that you can never know enough. To truly defeat an enemy you must first understand and study it. Only then will you have the tools to defeat it. Thus I ask you again to please take 49 minutes out of your day to view the program *Chasing the Dragon: The Life of an Opiate Addict* (viewer discretion advised due to strong language and graphic images). This film can be viewed at www.FBI.gov/ChasingTheDragon.

According to the Drug Enforcement Administration (DEA), three out of four heroin users started by abusing prescription pills. Medical experts will tell you that opioids in a bottle are no different than the heroin you buy in a glassine bag. The majority of persons have a medicine cabinet somewhere in their home. Most parents I know lock their wine/beer coolers in their home in order to remove the temptation from their kids. If they cannot access it, they will not drink it. So, why do we keep dangerous pain killers in medicine cabinets that are

accessible to our children? If you do not need them, get rid of them. If you are taking them, then lock them up. If you do not know how to get rid of them, use the internet. There are several safe ways to dispose of unused prescription drugs.

I know I am repeating myself, but, I should not have to. Several times each year the DEA sponsors a drug take-back program across the U.S. and every time several tons of unused pills are turned in. The DEA also reports that the U.S. makes up less than 5 percent of the world's population, but we consume 80 percent of the opioids manufactured in the world. Again, I am not saying you may not need these drugs to fight chronic pain. All I am saying is do not be the cause of a family member's curiosity that can potentially lead to addiction and death.

One of the most rewarding parts of my job is meeting the public when I do public speaking on drug identification and drug awareness. I have attended countless parent-teacher association (PTA) meetings. The saddest realization I am always faced with is the lack of attendance by parents. I go to PTAs at the request of the schools and parents, but when I attend a school with over 1,500 students, only seven parents attend and this has happened all too often. I recently attended one where none of the parents attended and the film was shown to school staff only.

I would implore you to not be the next family used to make the next heroin documentary and to not be the next person interviewed because of your addiction. Also, do not be the one who gets the call in the middle of the night from the police letting you know that your child has died from an overdose.

IS THERE HOPE?

Naloxone, also called Narcan, was patented in 1961 and its use was approved by the Food and Drug Administration in 1971. It is used to block the effects of an

opioid that would otherwise lead to an overdose. It has been described as the wonder drug or the lifesaving drug and it has saved countless lives across the U.S. It was until recently only available by prescription. This is now changing throughout the nation. When administered it will counteract the opioid overdose within minutes. Does it work all the time? Unfortunately not. In some cases, the overdose victim just cannot be revived. However, there are more success stories than failures. The Fairfax County fire department has saved many lives. I know this firsthand, since I am contacted about every overdose case that occurs in our county. Time after time I am told that Narcan was administered with the desired effect (the victim is alive).

Police and Sheriff Departments are beginning to carry Narcan as a daily tool to help keep people alive. Parents are attending Revive training to save their children's lives in the event of an overdose. Churches are promoting it and in Fairfax County a sister who lost her brother is a strong advocate for it. Ginny (Atwood) Lovitt started the Chris Atwood Foundation. I encourage you to go to <http://www.chrisatwoodfoundation.org/>, read her story, learn about Naloxone/Narcan and see how you can help.

When it comes to Naloxone/Narcan, I have asked that a warning label be placed on the prescription or on the drug itself, such as the warning label on a pack of cigarettes. This drug is not a cure for addiction. I have seen users with an ample supply to ensure they stay alive to continue chasing that high, but I will never be the one to say, "Do not use it." However, I will say, "If you have cheated death once. It is time to seek help."

On April 6, 2017, I attended a summit put on by the Police Executive Research Forum held at the New York City Police Headquarters. The summit, "Responding to the Opioid Epidemic," was attended by law enforcement from across the U.S. and Canada. It was also attended by the Drug Enforcement Administration, the Office for National Drug Control Policy, community services, health professionals, prosecutors, chiefs of police and sheriffs. Each participating agency shared how they were dealing with the current crisis.

The federal government understands the current epidemic facing the U.S. More U.S. dollars are being spent to combat this plague. Different rehabilitation treatments are available and more bed spaces are being created. There is hope.

FINANCIAL INSTITUTIONS (FIS) CAN HELP IN SO MANY WAYS

First and foremost, there is the suspicious activity report that has been talked about and discussed so many times. When I speak to financial institutions, I always ask them to think about the big picture and to always apply commonsense at work. For instance, if a doctor banks with your institution, what is their normal deposit? Did a sudden change take place where large cash deposits are suddenly being made? There are doctors out there who sell prescriptions for the right price. However, there are bad apples in every profession. Recognizing them is where educating yourself comes into play.

Fentanyl and carfentanil are manufactured in legitimate labs. They are also manufactured in illegitimate labs. When a company opens an account with your institution and provides an address for the business, does someone search the address on the internet, use a map engine to get a satellite look at it, and/or get an onsite inspection of the company?

When dealing with a correspondent bank, you are told that all the homework has been done and that customer due diligence (CDD) has been completed. Do you take them at their word or do you do your own homework to protect the integrity of your institution?

A local financial branch is probably not going to identify a heroin user due to the several withdrawals conducted at an ATM. Most of the time heroin users have depleted their life savings buying illegal drugs. However, dealers are a different story. For example, take the case of John the drug dealer (this is a recent case still going through the justice system, so his name has been changed). John enters a financial institution and opens a business account under the name "John's distribution services, LLC." He provides a fictitious business address and begins to sell heroin and cocaine. He then makes cash deposits under the reporting requirement. He is arrested and his

bank statement is found in his car at the time of his arrest. CDD and know your customer can help save a life. This dealer was selling a lot of heroin for some time before he was caught. Just a point (tenth of a gram) of heroin can cause an overdose and death.

I spoke about this case at an ACAMS U.S. Capital Chapter event and was asked what led to this person's arrest. Old fashioned police work, surveillance, heroin purchases and our police helicopter. This individual was followed several times to establish a pattern of his selling habits. This also enabled us to identify several purchasers/users in our county. Our police helicopter assisted us the aerial surveillance, which led to the discovery of a bank in Washington, D.C. Our Street Crimes Unit was called on to make an arrest after he sold heroin. The arrest was conducted to perfection and a search incident to the arrest led to the discovery of cocaine, heroin and financial records. A search warrant was executed at his home in Washington, D.C. by the U.S. Park Police (partnerships). They found cocaine, heroin and firearms. John has pled guilty to numerous counts of distribution in Fairfax County and is awaiting court on the federal charges on the items seized from his home.

I am also a strong proponent of forming partnerships between law enforcement and financial institutions. I am sure you have heard me say this time and time again in past articles or at conferences. How hard is it to pick up the phone and talk to your local police department or federal agency? Find out who is working in your area and set up a meeting. Hold a joint sharing of information, I know this sounds crazy, but it works. Only together can we strive to accomplish the goal of saving a life, protecting our home, protecting our community, protecting our institution, and most importantly passing on a better earth than the one we are living on now.

A PERSONAL NOTE


In my first article, I included the "My Safety Plan" that was enclosed in a packet with material on how to get help. As a police department, we passed this safety plan out to 120 people suffering from addiction. Out of those 120 packets provided, one person agreed to get help. That person thanked members of our

squad for saving her life. She was proud to share that she had been clean for almost a year, had regained custody of her three-year-old son and was now a manager at her business. She felt she had us to thank for saving her life.

This person invited us to her upcoming one-year anniversary of sobriety. It gave us renewed energy in battling this epidemic. We reached out to her to tell her story to a larger audience to let people know there is hope. After unsuccessfully reaching out to her we were notified she had died from a drug overdose.

My heroin group of detectives and I have seen too much death and misery caused by addiction. Families torn apart or destroyed, children suffering because their parents are addicts. As a society, I ask you again to research this increasing crisis in our world today. Become a volunteer to help end this epidemic. Talk to your family (children) about drugs and addiction. Do not ever think that this will never happen to you.

CONCLUSION

I did not think that the heroin epidemic could get any worse until the reintroduction of fentanyl and carfentanil. Now just a pure microgram of either drug can kill an unsuspecting law enforcement officer through accidental contact conducting a field test of an unknown white powder. More synthetic drugs are being created to avoid law enforcement detection and seizure. Our youth are living the Superman syndrome where they believe nothing will hurt them. People buying heroin take their local dealer's word that what they are buying is safe. However, to be on the safe side, dealers are now giving away free Narcan with their drug sale. A dead client is a bad client and it means that no money comes in. As a society we cannot let this epidemic continue to spread. Only through education and partnerships does our planet have any hope. 

James A. Cox III, CAMS, second lieutenant, Fairfax County Police Department, Fairfax, VA, USA, james.cox@fairfaxcounty.gov.

COMBATING CYBER FRAUD in CORRESPONDENT BANKING

Cybercrime is a major concern for banks around the world. Until recently, the focus of attacks has tended to be on banks' customers through card and account detail compromises. But as criminals have become more sophisticated, they have raised their ambitions, and in a change of focus are now directly targeting banks themselves. In light of these threats, what steps can financial institutions take to protect themselves from cyberattacks, detect suspicious activity more readily, and improve their chances of recovering quickly from any cybercrime attacks?



Current context

When looking to identify current threats, the first thing to understand is that organized cybercrime can take a number of different forms, ranging from a scatter-gun approach to sophisticated high-end, targeted attacks.

David Ferbrache, technical director for cybersecurity at KPMG U.K., explains that fraudsters typically start with commoditized attacks, whereby organized crime groups send millions of emails containing phishing links to malware. "If clicked on, these can result in the system being compromised and the potential for money to be extorted by ransomware demands," explains Ferbrache. "Only a small number of these attacks prove successful, but it's a numbers game."

The second stage is tailored or targeted attacks. As Ferbrache explains, "The organized crime groups spend a couple of weeks researching the organization they want to compromise, and the phishing attacks they undertake are just that bit more credible, targeted and specific." One example of this is business email compromise schemes, which have already led to losses of over \$3 billion, according to figures published by the FBI in June 2016.¹

Sophisticated fraudsters are now mounting focused high-end attacks. Organized crime groups have begun directly targeting bank systems. Unlimited cash-out attacks, for example, have seen criminals compromise the networks of card-issuing banks, enabling

¹ "Business E-mail Compromise: The 3.1 Billion Dollar Scam," FBI, June 14, 2016, <https://www.ic3.gov/media/2016/160614.aspx>



Organized crime groups have begun directly targeting bank systems

them to modify withdrawal limits and clean out groups of ATMs in coordinated assaults.² Ferbrache says that one notable attack in 2013 saw a \$40 million loss across 24 different countries in a single night.

In other cases, malicious software is uploaded to ATMs through banks networks, so that the machines respond to codes entered by the organized crime groups. Last year, such attacks were carried out in countries including Taiwan, Thailand, Russia, Armenia, Belorussia, Poland, Germany, Georgia, Romania, Kyrgyzstan, Estonia, Spain, the Netherlands, the U.K. and Malaysia.

Last year's attack on the Bank of Bangladesh, which resulted in the loss of \$81 million, is of particular concern to correspondent banks. While the attack itself took place in early February 2016, the ultimate beneficiary accounts in the Philippines had allegedly been opened a year earlier, which is likely to have been when the attackers began their initial reconnaissance. Software on the bank's interface server was modified, not only to enter fraudulent payment requests, but also to conceal this activity so that fraudulent transactions would not appear on daily logs.

The shift from targeting banks' customers to targeting banks themselves represents a very significant change

Preventing and detecting attacks

The shift from targeting banks' customers to targeting banks themselves represents a very significant change and an increasing threat to the correspondent and the wider banking community. However, it is important to note that while compromises have taken place in banks' own environments, there is no evidence that the SWIFT network and core messaging services were compromised in any of the attacks.

The attackers are very well organized and sophisticated in terms of how they carry out back-office attacks. They follow a four-step process:

1. Compromising the customer's environment, introducing malware using techniques such as phishing or email compromise scams.
2. Capturing valid operator credentials, typically through access to password files or by putting keyloggers in place to capture password details, and thereby gaining an understanding of the payment environment and associated behaviors.
3. Using fraudulent credentials to attack the back office; for example, by sending fraudulent MT 103 payment messages.
4. Hiding transaction activity. For example, by removing payment information from local databases, modifying incoming statement information or rendering the local environments inoperable and thereby delaying the discovery of the attack and increasingly the likelihood that funds will be settled.

² Chris Strohm, "Most-Wanted Cybercriminal Extradited to U.S. From Germany," *Bloomberg*, June 23, 2015, <https://www.bloomberg.com/politics/articles/2015-06-23/turkish-man-accused-in-global-atm-heist-extradited-to-u-s>



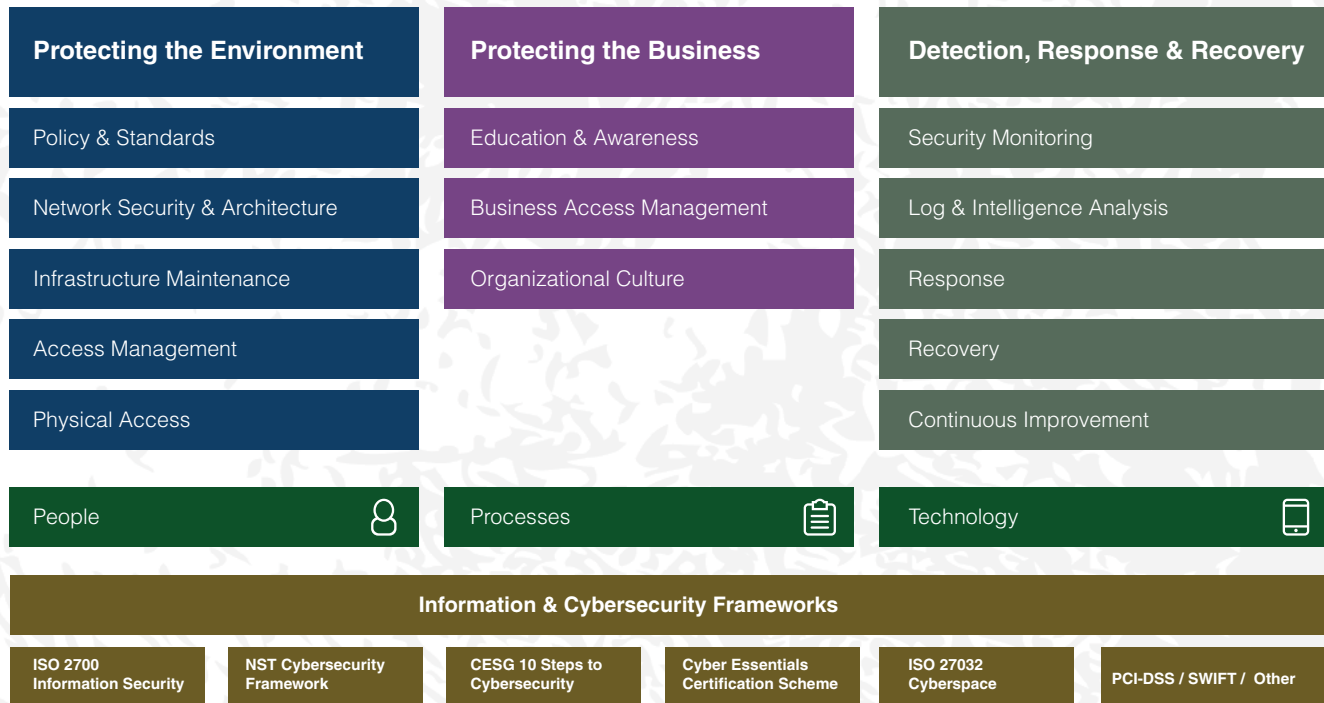


Table 1: Cybersecurity Best Practice Considerations

As attackers begin to understand banks' internal processes and infrastructure, it is clear that they are becoming more dangerous. As such, there is a greater need for financial institutions to take steps to protect their key systems and gateways.

While financial institutions would ideally be able to prevent any cyberattack from taking place, it is impossible to eliminate the threat entirely. As well as putting controls in place to prevent attacks, institutions need to be able to detect attacks when they occur, and should prepare recovery and response procedures.

From information sharing across the banking community to the adoption of appropriate market practice, there are a number of tools, techniques and initiatives that can help banks mitigate the risks, identify suspicious activity and recover from incidents.

Establishing a strong foundation

As cyberattacks become more prevalent, the industry and regulators are taking steps to understand, address and mitigate the risk. In May 2016, SWIFT launched its Customer Security Programme to strengthen existing cyber controls and provide a collaborative framework for its 11,000+ member institutions to manage evolving cyber threats. The Programme focuses on the need for institutions to secure and protect their own environments and share information within the SWIFT community, as well as the importance of managing relationships with counterparts.

SWIFT's initiative comes at a time where there is also increasing scrutiny and guidance on banks' cybersecurity from regulators. For example, in September

2016, the New York State Department of Financial Services (DFS) issued a proposal building on existing guidance in relation to cybersecurity.

A common feature of all of these approaches is the need to get basic security hygiene in place. While cyberattacks are becoming more sophisticated, the importance of getting basic security right should not be underestimated. As show in Table 1, the following areas should be addressed:

- *Protecting the environment*— This includes defining and applying the appropriate policies and standards, as well as access management, and putting suitable security measures in place for the institution's network and architecture. Institutions should also apply measures such as segregating duties across key staff,

A bank might send the following MT 103 Single Customer Credit Transfer which is subsequently discovered to be fraudulent:

From: Sender BIC
103
To: Receiver BIC

:20:1234567890
:23B:CRED
:32A:160910EUR800000,00
:50F:/942267890
1/FRAZ HOLZAPFEL GMBH
2/GELBSTRASSE, 13
3/AT/VIENNA
:57A:BANKGB22
:59:/9876
A. FRAUDSTER
1, CROOKED STREET
LONDON
:71A:SHA

The following MT 192 should be sent as soon as possible to the recipient of the MT 103:

From: Sender BIC
192
To: Receiver BIC

:20:ABC123
:21:1234567890
:11S:103
:160809
:79:/FRAD/
:20:1234567890
:23B:CRED
:32A:160810EUR800000,00
:50F:/942267890
1/FRAZ HOLZAPFEL GMBH
2/GELBSTRASSE, 13
3/AT/VIENNA
:57A:BANKGB22
:59:/9876
A. FRAUDSTER
1, CROOKED STREET
LONDON
:71A:SHA

If the original message is not available in FIN format, a full description should be provided as follows:

From: Sender BIC
192
To: Receiver BIC

:20:ABC123
:21:1234567890
:11S:103
:160809
:79:/FRAD/
Payment of EUR 800000,00
value dated August 10.
Ordering Customer
/942267890
1/FRAZ HOLZAPFEL GMBH
2/GELBSTRASSE, 13
3/AT/VIENNA
Beneficiary Bank
BANKGB22
Beneficiary Customer
/9876
A. FRAUDSTER
1, CROOKED STREET
LONDON

- Field 20 of the message believed fraudulent
- The message was an MT 103...
- ...sent on 9th August 2016
- Cancellation request relates to a fraud
- Copy of the original message details

- Field 20 of the message believed fraudulent
- The message was an MT 103...
- ...sent on 9th August 2016
- Cancellation request relates to a fraud
- Description of the transaction including beneficiary, beneficiary bank, and account

Using the correct SWIFT message format can increase the likelihood of successfully canceling payment transactions when fraud is suspected.

- dealing appropriately with new and departing staff and controlling privileged access to systems.
- *Protecting the business*— In some cases, institutions may focus on cybersecurity without necessarily understanding the business context. Research has indicated that a majority of SWIFT customers see human factors as the greatest area of weakness where cyber threats are concerned. Therefore, education is critical when it comes to raising awareness of current threats. In some cases, institutions use simulated phishing messages within their organizations so that they can identify the need for reinforcement training if staff click on malicious links.
 - *Detection, response and recovery*— Institutions should ensure that the required security monitoring measures are in place, such as continuous policy monitoring

and the use of proper processes to monitor critical events. Specific measures should also be put in place, such as reviewing relationship management applications (RMAs) and adopting relevant market practice.

Reviewing RMAs

When it comes to managing relationships with counterparts, there are a number of steps that financial institutions can take. The first is to review the relationships covered by the RMA.

RMAs are 'digital handshakes' between financial institutions that specify whether transactions can be exchanged. Without an RMA in place, institutions cannot receive SWIFT messages from counterparts. Using RMA Plus, banks can exercise further control by specifying which particular types of messages they wish to exchange over the network and with whom. Therefore, RMA and RMA Plus enable banks to mitigate risk by

avoiding the sending and receiving of unwanted messages and reducing the risk that someone within either institution initiates unauthorized transactions.

However, transaction patterns can change over time. As a result, as many as 60 percent of RMA relationships are dormant or inactive, meaning that institutions may be needlessly exposing themselves to particular corridors. Superfluous RMAs can also result in unnecessary costs, as compliance requirements will often dictate that KYC reviews are carried out on counterparts with whom open RMAs are in place. As such, institutions should regularly review the RMAs they have in place, for both cost and security reasons.

Guidance published by the Wolfsberg Group last year noted that financial institutions "should incorporate RMA due diligence standards into their Financial Crime/AML/KYC programmes," for example, by segregating RMA requests between customer

relationships and non-customer RMAs. The guidance notes that “due diligence on the RMA holder should consider the message types used by the RMA holder and the risk associated with the activity conducted.”³

Market practice

There are other actions financial institutions can take in order to detect fraud more readily and respond more effectively to any threats. For example, it is good practice to reconcile accounts, provide payment confirmation and have policies in place around payment amendments. Institutions should also know how to cancel payments rapidly, should the need arise.

One step that institutions can take is to send—and require counterparts to send—SWIFT MT 900 and MT 910 confirmation messages. While these messages are not currently mandatory, they provide additional transparency between counterparties. By the same token, banks should also review the MT 940/MT 950 statement messages that they receive in order to check that the amounts and balances recorded on their statements match their own records of transaction activity.

As a further step, banks should avoid the use of free format messages such as MT 199 to amend or change payment instructions, as this can impede reconciliation. Instead, banks should cancel the original instructions or send payment adjustments if payment instructions need to be changed or canceled.

Monitoring transaction data

Given the growing tendency of cybercriminals to conceal their fraudulent activity, banks should also carry out activity monitoring and risk monitoring, both to prevent fraud and to detect attacks that do take place.

- *Activity monitoring*—By obtaining an aggregated record of daily activity, banks can gain a clearer understanding of their payment activity and identify any significant changes in activity.
- *Risk monitoring*—By monitoring risk in their transaction environments, banks can counteract fraudsters’ efforts to hide their transaction activity, as well as identifying unusual single or aggregated transactions.

Institutions should source and store such information separately to ensure that it cannot be compromised in an attack that disables or damages their own payment systems and records.

Response and recovery

It is also important to have robust processes in place so that financial institutions can respond quickly and effectively if they detect a cyberattack. This may involve canceling fraudulent messages, or taking steps to facilitate business continuity if transactions cannot be canceled.

Canceling fraudulent transactions

In some cases, it may be possible to cancel a fraudulent instruction by sending a cancellation message. In order to cancel a payment instruction, banks should immediately send an MT n92, where ‘n’ refers to the category of the original message. For example, an MT 103 would require a MT 192 cancellation message, and an MT 202 would require an MT 292.


When using a cancellation message, it is also important to use the correct fraud code, as this is used to prioritize the request and improve the likelihood that the instruction will be successfully canceled. The required code is the use of the code word /FRAD/ in field 79 of the cancellation message.

Disaster recovery/business continuity

As the final stage of defense, financial institutions need to have measures in place that enable them to respond appropriately to cyberattacks and restore usual business operations as quickly as possible. This requires a strong link between cybersecurity and business continuity/disaster recovery, as well as an understanding that cybersecurity is intrinsically connected to the core business. “Cyber is not something you can separate from the core business,” comments Ferbrache. “All of our businesses are digitally dependent now, and all of them deal with digital threats.”

In order to have effective recovery processes in place, institutions should have worked through different scenarios and understood their consequences. Institutions need to plan how they will contain or mitigate the consequences of an attack, as well as knowing how they will deal with communications, regulatory and legal issues. They also need to have a plan in place stating how they will bring the business back online quickly and securely.

Conclusion

As cybercriminals turn their attention deeper into the banking world, it is imperative that financial institutions take appropriate steps to secure their environments. There are a number of areas in which actions can be taken both to prevent attacks, as well as to increase the likelihood of an attack being detected in time. Last but not least, institutions need to have a clear business continuity plan in place covering the steps to take in the event of a successful attack. 

*Tony Wicks, head of AML initiatives, SWIFT, London, U.K.,
tony.wicks@swift.com*

³ “Wolfsberg Guidance on SWIFT Relationship Management Application (RMA) Due Diligence,” the Wolfsberg Group, <http://www.wolfsberg-principles.com/pdf/standards/SWIFT-RMA-Due-Diligence.pdf>

Ethically enhanced due diligence and human trafficking



In 2016, *ACAMS Today* published the article, “Raising Awareness About Human Trafficking,” which talked to the value of public-private partnerships and a Canadian anti-human trafficking initiative called Project Protect.¹

As a result of Project Protect, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has identified that suspicious transaction reports (STRs) received during 2016 had increased by 500 per cent over the previous year and by extension disclosures to law enforcement by 537 percent.

FINTRAC, working closely with the private sector, law enforcement and victims of human trafficking also published a comprehensive operational alert, which was circulated to 31,000 law enforcement agencies and reporting entities.² The alert focused on indicators of money laundering related to human trafficking as sexual slavery, and complements the 2014 FinCEN guidance on human trafficking, which also addresses human smuggling and trafficking for labor exploitation.³

Last year was globally catalytic in raising awareness on human trafficking, with awareness now being translated into action that addresses the problem using a multifaceted approach, albeit arguably often in a patchwork quilt of well-intentioned, but often competing effort.

“A patchwork quilt” should not be seen as a criticism, rather as groundswell recognition of the inhumanity of human trafficking and a desire to end it across its multiple fronts (sex trafficking, labor trafficking, organ trafficking, etc.) accompanied by multiple initiatives.

In Canada, examples of initiatives include numerous law enforcement agencies and nongovernmental organizations promoting human trafficking campaigns resulting in arrests and interdictions. For example, on April 11, London (Ontario) Police announced the results of Project Equinox, which resulted in 78 arrests of traffickers and their clients and 18 victims of human trafficking being rescued from the clutches of their pimps, the youngest aged 15 years.⁴

In the U.S., *CNN* reported on “The Trucker Army” against human trafficking—big rig truckers on the lookout for and rescuing victims of human trafficking. In addition, various states including Texas, Kansas, Arkansas and Ohio, are enacting laws to require prospective truck drivers to undergo compulsory human trafficking awareness training.⁵

Internationally it is refreshing to see recent human trafficking arrests in places like Fiji and Kenya.^{6,7} In February 2017, Peter Warrack had the privilege of presenting on a project to combat human trafficking in the Caribbean as part of an Interpol training program held in St. Lucia. Also, human trafficking was on the agenda at a Financial Action Task Force (FATF) typologies meeting in Moscow on April 24, 2017.

In keeping with the global narrative, on March 15, 2017, the U.N. Secretary General António Guterres urged governments to implement laws to prosecute traffickers⁸ and called for governments, (and by extension law enforcement) to engage with the private sector and cautioned that any support

Last year was globally catalytic in raising awareness on human trafficking, with awareness now being translated into action that addresses the problem using a multifaceted approach

¹ Karla Monterrosa-Yancey, “Peter Warrack and Constable Lepa Jankovic: Raising Awareness about Human Trafficking,” *ACAMS Today*, June-August 2016, <http://www.acamstoday.org/warrack-jankovic-raising-awareness-human-trafficking/>

² “Indicators: The Laundering of Illicit Proceeds from Human Trafficking for Sexual Exploitation,” FINTRAC, December 15, 2016, <http://www.fintrac.gc.ca/publications/operation/oai-hts-eng.asp>

³ “Guidance on Recognizing Activity that May be Association with Human Smuggling and Human Trafficking—Financial Red Flags,” FinCEN, September 11, 2014, <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a008>

⁴ “London-Area Police Help 18 Women and Girls Leave Sex Trade after Human Trafficking Operation,” *CBC News*, April 11, 2017, <http://www.cbc.ca/news/canada/windsor/london-area-police-help-18-women-and-girls-leave-sex-trade-after-human-trafficking-operation-1.4065745>

⁵ Eoghan Macguire, “Eyes of the Highways: Raising a ‘Trucker Army’ for Trafficking Fight,” *CNN*, April 12, 2017, <https://amp-cnn-com.cdn.ampproject.org/c/s/amp.cnn.com/cnn/2017/04/12/world/truckers-human-trafficking-freedom-project/index.html>

⁶ Praneeta Prakash, “Cases of Human Trafficking in Fiji,” *Fiji Broadcasting Corporation*, April 6, 2017, <http://www.fbc.com.fj/fiji/49675/cases-of-human-trafficking-in-fiji>

⁷ “Seven Somali Men Arrested Over Human Trafficking Ring in Kenya,” *Eyewitness News*, April 6, 2017, <http://ewn.co.za/2017/04/06/7-somali-men-arrested-over-human-trafficking-ring-in-kenya>



needs to incorporate the voices and views of the people affected (i.e., the victims of human trafficking).

Working in partnership with the public sector is not new in Canada (as seen by Project Protect) and there are similar initiatives in the U.S. However, when the public and private sectors (Canada's FIU FINTRAC and a major bank) co-presented on the subject at the U.N. University event, Breaking the Financial Chains Workshop,⁹ held at Grace farms in Connecticut on April 2017, many in

the esteemed audience viewed this as positive, revolutionary and a takeaway to present back to the U.N.

The need for all stakeholders to work together in fighting all forms of human trafficking was a clear message in the RUSI¹⁰ report "Disrupting Human Trafficking: The Role of Financial Institutions" as presented by Tom Keatinge at the Grace Farms Workshop.

As the two-day workshop unfolded, it became clear that whilst Project Protect addressed human sex trafficking, other

forms of human trafficking not as prevalent in Canada (i.e., the issues of forced labor and supply chain due diligence) were of major concern to the international audience in attendance.

Standard Chartered Bank (Netherlands) provided a compelling presentation on supply chain due diligence centered on the diamond industry in the Democratic Republic of Congo.

In identifying the elements of the supply chain (i.e., production, distribution, preparation and sales), the presenter opined on increasing public and regulatory expectations that institutions providing financial services (e.g., banks) to entities in the supply chain would conduct due diligence on the customer's customer to provide a level of comfort that there was no association to human trafficking (or as in this example slavery and forced labor).

I refer to this as ethically enhanced due diligence (EEDD) and, according to lawyer, Michael Volkov, in an article published online on April 4, 2017:

"There are specific legal risks for U.S. companies that may arise from federal contracting regulations and possible AML implications. More important, is the reputational risk for global companies that may fail to implement basic hiring and employment controls to avoid human trafficking. Companies have to monitor and regulate their supply chains to avoid the serious harm from human trafficking and possible hiring or facilitation of hiring of human trafficking victims.

Since 2015, every company with a U.S. government contract must comply with U.S. regulations governing human trafficking. Companies that have a contract over \$500,000 must implement a specific compliance program and certify each year to compliance. Companies have to implement compliance programs to detect and prevent human trafficking by third-party agents and subcontractors that may recruit potential employees from overseas or may use

⁸ "At Security Council, UN Officials Urge Governments to Implement Rules on Prosecuting Traffickers," UN News Centre, March 15, 2017, <http://www.un.org/apps/news/story.asp?NewsID=56355#.WO46XS0rLIU>

⁹ <http://gracefarms.org/>

¹⁰ Royal United Services Institute—a U.K. Think Tank, https://rusi.org/sites/default/files/201703_rusi_disrupting_human_trafficking.pdf

such employees in overseas positions. This requirement extends to monitoring and auditing of third-party agents and subcontractors for compliance with human trafficking prohibitions.

Prime contractors are required to exercise vigilance in making sure that their subcontractors comply with specific contractual requirements.”¹¹

Volkov’s useful article alludes to possible AML implications, but does not spell them out. It would arguably make sense that if goods are manufactured using slave labor, which is a crime in many countries, then those goods and the funds derived from selling them become the proceeds of crime.

If the funds are then transmitted through the financial system, it is at this point where money laundering may occur and be reportable via a STR or suspicious activity report (SAR).

Ethical Due Diligence is gaining momentum internationally and is becoming further embedded into law, and by extension compliance. In February, Dutch legislators adopted a new bill, which if enacted would require certain companies to investigate the existence of child labor in their supply chain and on March 27, 2017, the French Parliament adopted a law establishing a duty of vigilance for parent and subcontracting companies. The law amends the Commerce Code and requires companies to establish and implement a plan for improving human rights, the environment, and health and safety issues in their supply chains.


Another takeaway from the U.N. University were findings from Liberty Asia, an NGO that “aims to prevent human trafficking through legal advocacy, technological interventions, and strategic collaborations in Southeast Asia.”¹² Liberty Asia reported that out of 18 countries surveyed only six had formal guidance issued from their respective FIUs on the topic of human trafficking.^{13,14} Furthermore, it was noted that many countries without formal guidance relied

on other guidance issued in other jurisdictions, primarily the U.S. However, it is likely that this appropriation of intelligence can see diminished results as not all indicators are constant across international borders.

In summary, it is an uncomfortable but realistic assumption that human trafficking, in its many different forms, is not going away any time soon. According to the Pope, in a message read out by the under secretary of the Migrants and Refugees Section of the Dicastery for Promoting Integral Human Development, to the Organization for Security and Cooperation in Europe (OSCE)’s 17th Alliance against Trafficking in Persons Conference, in Vienna, it is getting worse.

However, although it may be getting worse in many parts of the world with respect to migrant smuggling and forced labor situations, in North America, as far as human trafficking and sexual slavery are concerned, there is reason to be optimistic as the public is becoming more

aware and corresponding action by law enforcement is addressing it. This is good news, but more needs to be done.

ACAMS has always been at the forefront of raising awareness about human trafficking as evidenced by the human trafficking panel at the recent AML and Financial Crime conference in Florida and numerous publications and chapter events over the years. Let us keep the message alive. 

Peter Warrack, CAMS, CBP, CFE, director of AML advisory and compliance officer, Bank of Montreal, Toronto, Ontario, Canada, peter.warrack@bmo.com

Joseph Mari, CAMS, CBP, senior manager—major investigations team, AML FIU, Bank of Montreal, Toronto, Ontario, Canada, joseph.mari@bmo.com

Disclaimer: The views and opinions expressed in the article are solely those of the authors.

¹¹ “Human Trafficking and Smuggling—A Compliance Requirement,” JDSUPRA, <http://www.jdsupra.com/legalnews/human-trafficking-and-smuggling-a-41216/>

¹² <https://www.libertyasia.org/about/>

¹³ Australia, Cambodia, Canada, China, France, Hong Kong, India, Indonesia, Liechtenstein, Malaysia, New Zealand, Singapore, Switzerland, Thailand, Netherlands, United Kingdom, United States and Vietnam.

¹⁴ Australia, Canada, Thailand, Netherlands, United Kingdom and the United States.

STEMMING THE FLOW OF CYBERCRIME PAYMENTS

Cybercrime for profit is a global economy that causes most of our cybersecurity and fraud woes and it is a problem to which all anti-money laundering (AML) and financial sector professionals should pay close attention. It is adaptable, ingenious and lucrative, while imposing vast costs on us. It victimizes financial institutions and their customers, and it uses our financial system as a conduit to transmit illicit profits and payments. Cybercrime for profit also provides a foundation for many other types of cybercrime, including hacktivism and nation-state attacks.

Cybercrime exploits companies and individuals throughout the world and it is perpetrated from all over the world, victimizing and using financial institutions everywhere. Thus, it is important that the global community works together to fight cybercrime. The U.S. is one country that is a lucrative target and pipeline due to its wealth and robust financial sector.

Crime has existed since the dawn of civilization, but cybercrime presents a defining change. Previously, criminals needed physical proximity to the victim. Now, criminals can victimize institutions and individuals from afar and across international borders. This shift means a global pool of attackers, decreased odds of apprehension, increased profitability and reliance on the financial industry to perpetrate these crimes from afar. Traditionally, law enforcement plays a major role in keeping crime suppressed to a manageable level, but with cybercrime it has not yet gained such traction. All of this demonstrates the important role the financial sector can play in reducing cybercrime.

The immense profitability of cybercrime demonstrates the high cost of victimization and the massive amount of theft, but it also presents an opportunity. Law enforcement and the AML community can “follow the money” among the facilitators and to the ultimate perpetrators. Furthermore, cybercriminals commit these frauds because they make money

from them. Thus, finding a way to reduce the flow of the profits would make it less lucrative and it would reduce the size of the criminal economy.

When foreign-based cybercriminals commit cybercrime and fraud that victimizes the U.S., funds representing illicit profits are transmitted through and outside of the U.S. financial system, and into the hands of the cybercriminal. In order to detect and stem this flow, one must understand the cybercrime and identity theft economy (i.e., how the participants earn money and how they pay each other).

The cybercrime and identity theft economy

One of the first criminal investigations to explore the full nature of this global cybercrime economy was *People v. Western Express International, Inc.*, et al., a case brought against a corrupt digital currency exchanger and some customers who were cybercriminals and identity thieves.¹ Underpinning the case were valuable lessons that hold true today and teach us about:

- The relationship between international cybercriminals and domestic identity thieves
- The marketplace for stolen data and the crimes they are used for
- Value transfer methods to support the trafficking of stolen data

- Cybercrime money laundering techniques
- Methods cybercriminals and identity thieves use to achieve anonymity
- Methods to pierce veil of anonymity

Successful identity thieves and cybercriminals are good at what they do, reap considerable profits, maintain anonymity and evade law enforcement. However, this financial success provides evidence of both criminality and identity.

The key to reducing the cybercrime and identity theft economy is understanding it. The economy revolves around the theft of data, its resale and use to commit identity theft. Within the marketplace are many different actors, each performing different roles, all trying to make money. Many successful participants reside internationally, which means they need to rely on the U.S. financial system and U.S. participants to monetize cybercrime.

How cybercrimes are monetized internationally

Email account hacking

Email account hacking is a lucrative cyber fraud against which we should protect ourselves. Criminals might try to monetize a compromised email account through a simple scheme where the hacker sends a blast email to all of the victim's contacts:

¹ The investigation and prosecution spanned nearly a decade, most defendants pleaded guilty, while three proceeded to trial and were convicted of every count. See, e.g., Kim Zetter, “Ukrainian Carder in \$5 Million Ring Sentenced to 14-Plus Years in Prison,” *WIRED*, August 8, 2013, <https://www.wired.com/2013/08/carder-eskalibur-sentenced/>.

"Help, I'm stranded in [insert foreign city], please wire money ASAP."

"Don't try to call me because I lost my phone."

A greater threat is criminal use of a hacked email account to cleverly misdirect bank wires and steal the funds—representing an evolution of social engineering skills that has stolen hundreds of millions of dollars. Such scams are termed "business email compromise" fraud, "CEO fraud," or "CFO fraud," and every employee in the financial sector must be aware of them. Suppose Company A regularly receives invoices from Company B and then pays

by bank wire. A criminal hacks the email account of a Company B employee, impersonates that employee and sends an email to Company A, providing "new" bank wiring instructions. The employee in Company A is fooled and Company A wires funds to the "new" bank account, which is controlled by the fraudster who immediately wires the funds out of the country. The fraud can be quite sophisticated and believable, comes in variations that do not require email account hacking, and the scam can deceive victims to delay detection for days or weeks. This fraud directly affects the conventional financial

system as it uses traditional bank accounts and bank wires to steal, launder and send funds out of the country.

Payment card fraud

Payment card fraud requires many participants, and each needs to get paid for their part in making the fraud possible. This fraud relies on three basic steps that are depicted in Figure 1:

1. The theft of credit card data, such as through the data breach of a retailer
2. The sale of this stolen data to identity thieves
3. The use of this stolen data to commit fraud

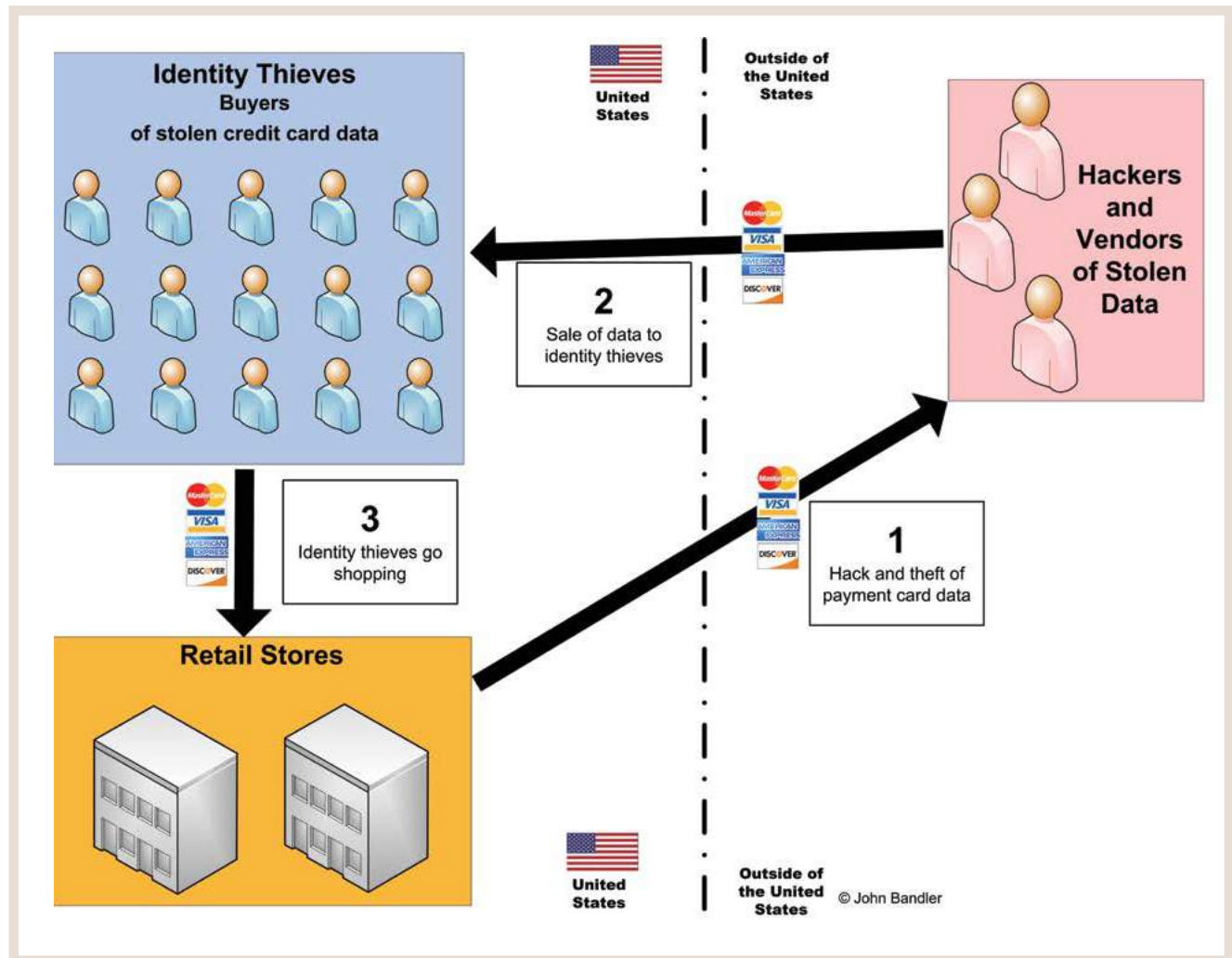


Figure 1: Payment Card Fraud

Here, the hacker is located outside of the U.S., and steals data pertaining to millions of credit card accounts from a retailer in the U.S. Stealing this data does not itself earn money for the criminal, so he must sell it to others to make money. Since this data was stolen from the U.S., the best market for this data is identity thieves in the country, since attempting to use these payment cards in foreign countries would likely trigger fraud alerts.

The identity thieves pay for this stolen data in a manner that maintains anonymity, and each payment may be small, a few hundred or thousand dollars. Payment could be sent through a money transfer service while using fictitious sender and recipient names or it could be sent via digital currency, such as Bitcoin, WebMoney and Perfect Money. Through these payments, a single vendor of stolen credit card data could earn millions of dollars per year.

Many other types of cybercrime fraud that exist ultimately require payment or transfer of funds from the U.S. to international cybercriminals based out of the country.

Moving the money

When sending and receiving payments, criminals—like legitimate business people—try to balance financial cost, convenience, speed and reliability. Criminals have the additional need for anonymity and secrecy. AML professionals should consider four basic conduits that cybercriminals use to move their funds:

- Bank wires through the conventional financial system
- Money transfer services
- Digital currency
- Money mules and shell corporations

Criminals have been misusing the financial system and payment methods since their respective creations. It should be no surprise that cybercriminals continue this trend and misuse whatever is available to them.

Bank wires

Bank wires, through the conventional financial system, remain an essential part of global funds transfer and are essential to the cybercrime economy. Financial institutions face a triple threat: 1) they are repeatedly attacked and risk becoming a fraud or data breach victim, 2) they need to prevent their customers from becoming fraud victims and 3) they need to prevent themselves from being used as an unwitting conduit for criminal funds or activity.

Bank wires might be initiated or misdirected based on fraud, including through the email account compromise scenario previously discussed. Banks have procedures to detect if the customer has been hacked, but sometimes procedures to detect other frauds are lacking. If the account holder relies on a third party who is hacked, or if the account holder is otherwise deceived or used as a tool for cybercrime-related fraud, banks might fail to detect it. Furthermore, some bank customers may use a variety of techniques to conceal the true ownership, source and destination of funds, including through money mule accounts and shell corporations. Bank wires also play a significant role with digital currency.

Money transfer services

Money transfer services, such as Western Union, are an important tool for identity thieves and cybercriminals, because it allows them to pay for stolen data, cybercrime services, and to purchase digital currency. To maintain anonymity, fake names are used when sending and receiving the payments. Successful cybercriminals earning millions of dollars per year may employ the services of other criminals to receive and process these money transfer payments. Occasionally, one recipient name becomes blocked because of associations with criminal conduct, in which case criminals can move on to another recipient name.

Digital currency

Digital currency has existed for two decades, and cybercriminals and identity thieves embraced it early on. The regulated digital currency industry is just a few years old. Though some digital currency proponents can be sensitive about its linkage with cybercrime, there are synergies that should be acknowledged and understood. They are ignored at the peril of the industry, since understanding makes it possible to keep the digital currency system clean, and thus ensure it is sustainable as a regulated industry.

Digital currency's connection to crime does not make it unique as a payment method. Consider how cash currency has been intertwined with traditional street crime, as with the drug trade. When illegal drugs are sold, the criminal transactions are in-person, and drugs are exchanged for cash. Successful drug dealers need to integrate mountains of cash into the financial system, and thus developed sophisticated money laundering schemes to make this possible. In contrast, cybercrime and data trafficking criminal transactions are completed online, and cash is inadequate. Payment needs to be made online, instantly and anonymously, in order for the stolen data to be delivered to the purchaser. Digital currency can do that; thus, it merely does for the cybercrime economy what cash does for the illegal drug economy. Compared to cash, there are both benefits and drawbacks for AML and law enforcement professionals.

Digital currency is affiliated with conventional banking and bank wires. Every digital currency exchanger needs a conventional bank account, and international bank wires are necessary to transmit funds in order to equalize the inherent trade imbalance that occurs when the cybercrime economy uses digital currency.

This digital currency trade imbalance occurs because there are identity thieves within the U.S. who continually purchase digital currency, which is then used to pay international cybercriminals for stolen data. This creates a

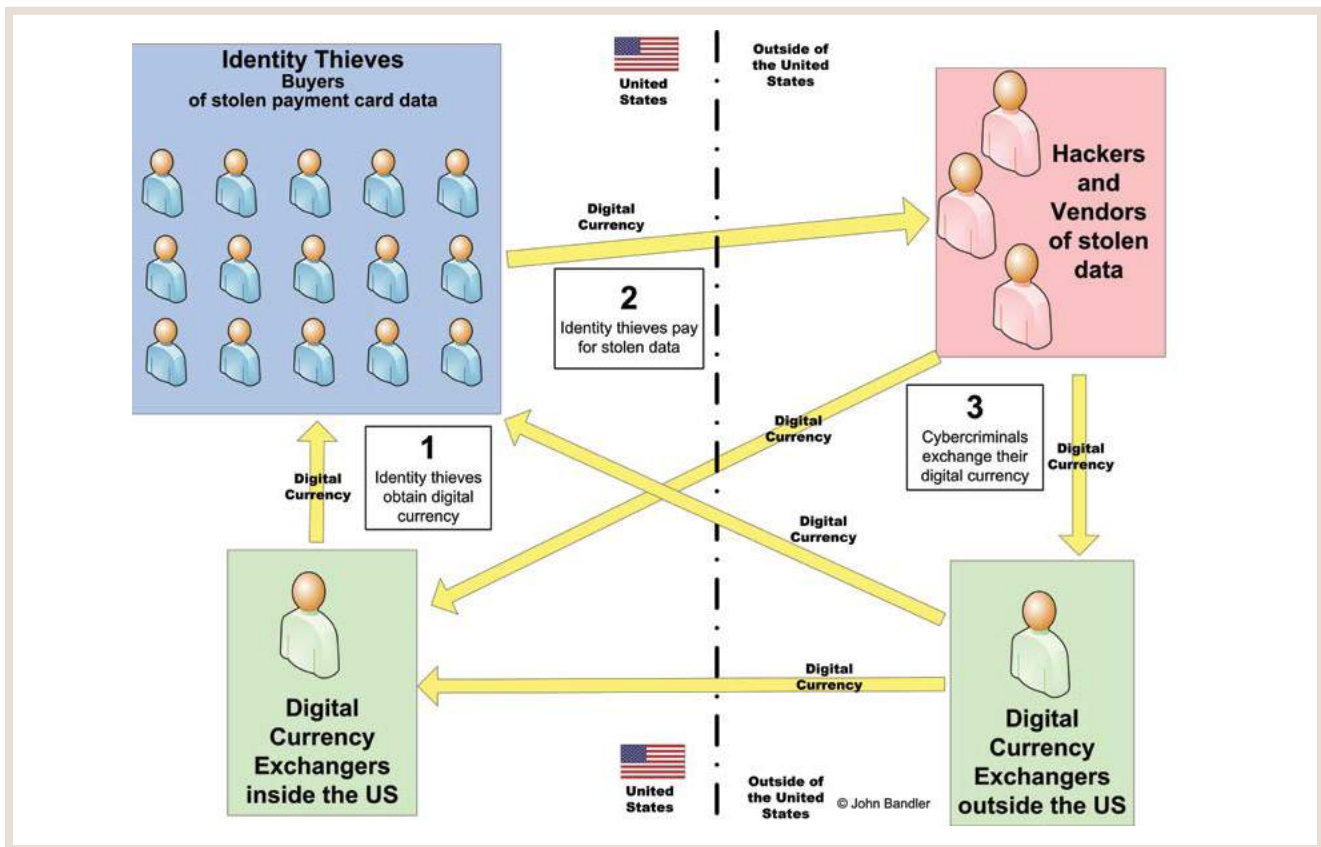


Figure 2: Digital Currency Repatriation

continual flow of digital currency payments from the U.S. to the destination country, and this digital currency needs to eventually be “repatriated” back to the U.S., so that it can be reused.

Consider Figure 2 and the basic steps depicted:

1. Identity thief obtains digital currency
2. Identity thief pays cybercriminal for stolen data
3. Cybercriminal exchanges digital currency for fiat currency
4. Repeat — identity thief needs more digital currency to buy more stolen data

The individual digital currency payments may be hundreds or thousands of dollars. In the aggregate, this represents an annual flow of millions of dollars.

Also, consider ransomware, an unchecked and lucrative fraud that also relies on digital currency, earning international cybercriminals millions of dollars per year. Ransomware is malware that infects a user’s computer and then encrypts the user’s data and holds it hostage, unless and until payment is made by digital currency from the victim to the fraudster. Thousands of ransomware victims purchase digital currency, which they then pay to international cybercriminals.

All of these digital currency payments to international cybercriminals create a digital currency trade imbalance, which is cured through repatriation of this digital currency back to the U.S. This return of digital currency can be accomplished through aggregate transactions of digital currency, with reciprocal bank wires from U.S. accounts to international accounts in order to pay for this digital currency.

Money mules and shell corporations

Cybercriminals located internationally rely on institutions within the U.S. to receive and process payments. Where funds are stolen from victims in the U.S., and ultimately destined for cybercriminals overseas, a money mule provides a convenient waystation through which to deliver the funds. A money mule is essentially a witting or unwitting person who receives and then transmits illegally acquired funds.

Consider the email account compromise scam previously mentioned, where Company A thinks it is wiring funds to Company B’s “new” bank account, but instead is wiring it to a money mule account, under the control of the fraudster. Company A is fooled by this fraud because the money mule’s account is within the U.S. If Company A had been told to wire the funds internationally, they would have known it was a fraud,

because Company B would not use a foreign bank account. Thus, the domestic money mule account is required to receive the funds, which can then be wired internationally. By the time the fraud is detected, the funds are outside of the U.S. and cannot be recovered. There are many ways through which money mules are recruited. Some crude, some quite sophisticated, backstopped with legitimate looking corporate identities, websites and documents.

Though money mules are often “disposable” (used for a single incidence of fraud and then cast away by the cybercriminal), there are more permanent waystations for funds. Shell corporations (or shelf corporations) and their bank accounts require more setup and management, and thus are less disposable. The underlying purpose remains the same: to disguise the true purpose of the account and the true owners. Once fraud or money laundering is detected, it is difficult for regulators and law enforcement to identify the ultimate beneficiaries of the fraud.

Every unsuspecting person is an avenue through which criminals can compromise computer or financial systems

Stemming the flow

Stemming the flow of cybercrime funds requires emphasis in the following areas:

- Personal cybersecurity and fraud awareness
- Increased review and scrutiny by the financial system
- Increased payments scrutiny

Personal cybersecurity and fraud awareness

Cybersecurity and anti-fraud is not just for experts, but an individual responsibility, like putting on a seatbelt or lock-

ing your front door at night. Every unsuspecting person is an avenue through which criminals can compromise computer or financial systems. This starts with each person at home, which protects the individual and family, and then extends to the organization. Each person can transform from being a potential attack victim to a detection sensor.

You should harden yourself by employing basic cybersecurity steps:

- Enable two-factor authentication (two-step login) on financial, email and other important online accounts
- Ensure your computing devices are kept malware free and updated
- Back up your data regularly and store it offline
- Do not open suspicious attachments or click on suspicious links
- Have verbal conversations to confirm any payment instructions
- Use common sense

Increased review and scrutiny by the financial system

The financial system faces the triple threats previously discussed, and is well suited to combat cybercrime funds transfer because of their resident expertise, systems and access to significant datasets. The financial system is ultimately the conduit through which aggregate cybercrime profits exit the U.S., so deeper analysis can help identify that.

Cybercriminals will continue to find victims and money mules within the populace of the U.S., and financial institutions should use their expertise in fraud and money laundering detection to identify these situations and stop illicit funds from exiting the country. Certain countries and banks are more likely to receive cybercrime fraud derived funds, and have proven uncooperative about tracing or recovering stolen funds. Overseas wires to such destinations should be scrutinized carefully before they are sent, because they are not recoverable once they are sent.

Increased payments scrutiny

International money transfers for the purpose of purchasing stolen data follow discernable patterns, even when

fictitious names are used by the sender and recipient. With enough data and experience, it is possible to distinguish criminal payments from legitimate payments. Similarly, though many digital currency accounts may be anonymous, payments can still be analyzed to discern criminal purposes. Furthermore, patterns indicating repatriation of digital currency to the U.S. should be closely researched.

The advent of digital currency regulation within the U.S. brought know your customer (KYC) requirements to domestic digital currency exchangers, meaning identity thieves may be inclined to use exchangers located outside the country. Thus, international money transfers can be used to purchase digital currency, and those patterns should be analyzed.

KYC methods that rely on telephone or online identity verification have inherent weaknesses when it comes to identity thieves and cybercriminals. These criminals have nearly unlimited access to stolen personal identifiable information, thus the mere provision of pedigree such as name, address, birthdate and social security number may be of limited use to confirm identity. In addition, if a payments company identifies suspicious activity and merely blocks payments to one criminal alias, the criminal will merely establish another. Thus, deeper analysis and a deeper remedy may be required. Finally, the ability of these criminals to make convincing forged identifications must also be considered, whether the identifications are presented online or in person.

Conclusion

Our collective steps as citizens of the world to combat the cybercrime epidemic have not been adequate yet, and there is room for improvement on many fronts. The financial and AML communities should recognize the crucial role they can play in this fight, and should work to reduce the flood of ill-gotten gains that criminals earn from these crimes. **FA**

John Bandler, Esq., CAMS, founder, Bandler Law Firm PLLC and Bandler Group LLC, New York, NY, johnbandler@bandlergroup.com

CYBERSECURITY: INDICATORS OF COMPROMISE

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) recently issued an advisory to financial institutions on cyber-events and cyber-enabled crime,¹ along with frequently asked questions.²

FinCEN's advisory encourages the preparation of suspicious activity reports (SARs) that evidence significant electronic activity and behavior, which prompts a timely review of challenges associated with three data points: Internet Protocol (IP) addresses (which serve as unique internet connection identifiers for online computers or servers), other online identifiers and Indicators of Compromise (IOCs).

IP addresses

Various websites are publicly available for internet users to look up their own IP address—whether it is dynamic (changeable) or static (fixed)—and IP addresses of other internet users.³

Demand for IP addresses has skyrocketed, given surges in growth for social media and Internet of Things connectivity for handheld and other devices. This demand is being met by IP addresses that are longer and more complex, requiring greater attention to accuracy when they are reported in SARs. The more familiar IPv4 32-bit numeric IP address scheme is being replaced by a longer IPv6 128-bit alphanumeric IP address scheme.⁴

The IPv4 address scheme supports 4,294,967,296 unique addresses and it uses the format nnn.nnn.nnn.nnn (n = number) with periods between segments. In contrast, the emerging IPv6 address scheme supports 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses and it uses the format cccc:cccc:cccc:cccc:cccc:cccc:cccc:ccc (c = character) with colons between segments, some of which are alphanumeric. Reportedly, up to 99 IP addresses in either format may be entered into FinCEN SAR form item 44.⁵

The accuracy of IP address geolocation tracking is relevant to a recent federal lawsuit. Plaintiffs allege that about 600 million IP addresses are mistakenly associated with their rural Kansas farm that is near the geographical center of the U.S. This mistake has led to plaintiffs alleging that they have been unfairly investigated for runaway children, attempted suicides, child pornography, and computer fraud and email spam.⁶ A federal judge recently denied the defendant's motion to dismiss.⁷

¹ "FIN-2016-A005 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," *United States Department of the Treasury - Financial Crimes Enforcement Network*, October 25, 2016, https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

² "Frequently Asked Questions (FAQs)," *United States Department of the Treasury - Financial Crimes Enforcement Network*, October 25, 2016, https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF

³ *WhatIsMyIPAddress.com*, <http://whatismyipaddress.com>

⁴ John D. Schanz, "How IPv6 lays the foundation for a smarter network," *Network World*, June 27, 2016, <http://www.networkworld.com/article/3088322/internet/how-ipv6-lays-the-foundation-for-a-smarter-network.html>

⁵ "FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions," Version 1.2, *Financial Crimes Enforcement Network*, October 2012, <https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf>

⁶ Complaint, James and Theresa Arnold vs. MaxMind, Inc., *United States District Court for the District of Kansas*, August 5, 2016, <https://consumermediallc.files.wordpress.com/2016/08/gov-uscourts-ksd-null-null-0.pdf>

⁷ Memorandum and Order, James and Theresa Arnold vs. MaxMind, Inc., No. 16-1309-JTM, *United States District Court for the District of Kansas*, October 20, 2016, https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2016cv1309-16

This Kansas farm case was cited by the Electronic Frontier Foundation (EFF), when challenging reliance on IP addresses to identify the location of crimes and the identity of individuals involved. EFF recommendations to law enforcement and the courts encourage proper evaluation of IP address data and early corroboration.⁸

Fraudulent IP addresses have been central to the Methbot botnet that is associated with losses exceeding \$180 million. Methbot uses U.S.- and Netherlands-hosted servers to power more than 850,000 bots with falsely registered IP addresses, which allowed cybercriminals to carry out the largest ad fraud scheme ever discovered. This scam reportedly yielded \$3 to \$5 million per day in fraudulent ad revenue by fraudulently obtaining IP addresses from overseas internet registries, and then registering them falsely to U.S. internet service providers. The IP addresses evaded fraud detection by appearing to originate from real users in the U.S.⁹

IP addresses are generally associated with a specific computer or server, but they may or may not be associated with an individual user, which could lead to data privacy concerns. Federal Trade Commission (FTC) officials regard the IP address as personally identifiable information that should be protected appropriately when it, or other persistent identifiers, may be linked to a particular individual, computer or device.¹⁰

FTC officials have cautioned website operators that collect persistent identifiers against making general statements that personal information is not being collected or that collected data is anonymous. Data protection measures and risk assessments should be appropriate to all collected data, not just data like the individual's name or email address.¹¹

The Court of Justice for the European Union (EU)¹² recently ruled that a dynamic IP address may be classified as personal data when combined with identifiable data about the individual user.¹³ This is consistent with the EU General Data Protection Regulation (GDPR), which will apply to EU countries on May 25, 2018.

GDPR Recital 30 states that natural persons may be associated with online identifiers, such as IP addresses. Such online identifiers may leave traces which, when combined with unique identifiers and other information received by servers, may be used to create profiles of natural persons and identify them.¹⁴

Website operators and app providers that collect EU personal data—on local or cloud servers¹⁵—should check on how IP address collection might be affected by GDPR requirements. This could include stricter consent, retention and cross-border data transfer obligations, although exceptions may apply.¹⁶

Countries like Argentina,¹⁷ Canada,¹⁸ Hong Kong,¹⁹ Japan²⁰ and Switzerland²¹ classify IP addresses as personal data when combined with identifiable data.

Brazil takes a notable approach with IP addresses. To facilitate the identification of users who have been engaged in criminal acts or personal data infringement, Brazil requires retention of user IP addresses in connection logs (which track the user's internet connection) and application access logs (which track the user's internet application use). Connection logs must be retained in a secure environment for one year and application access logs for six months. Police or administrative authorities may require longer log retention periods. Users must be informed about data protection and log retention practices.²²

Since October 2012, the Federal Bureau of Investigation, the Department of Homeland Security and other federal

⁸ Aaron Mackey, Seth Schoen, Cindy Cohn, "Unreliable Informants: IP Addresses, Digital Tips and Police Raids," Electronic Frontier Foundation, September 2016, https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf

⁹ "The Methbot Operation," *White Ops*, December 20, 2016, http://go.whiteops.com/rs/179-SQE-823/images/WO_Methbot_Operation_WP.pdf

¹⁰ "Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control, Keynote Address of FTC Chairwoman Edith Ramirez Technology Policy Institute Aspen Forum," *Federal Trade Commission*, August 22, 2016, https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf

¹¹ Jessica Rich, "Keeping Up with the Online Advertising Industry," *Federal Trade Commission*, April 21, 2016, <https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry>

¹² Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom

¹³ "Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland," *Judgment of the Court (Second Chamber)*, October 19, 2016, http://curia.europa.eu/juris/document/document_print.jsf?jsession...qMbN4PahaLe0?doclang=EN&text=&pageIndex=0&docid=184668&cid=90876

¹⁴ "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016," *Official Journal of the European Union*, April 5, 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

¹⁵ "Managing the Challenges of the Cloud Under the New EU General Data Protection Regulation," *Netskope*, 2016, <http://cloudfeurope.com/wp-content/uploads/sites/3/2016/05/Netskope-EU-GDPR-Managing-the-Challenges-of-Cloud-White-Paper.pdf>

¹⁶ Alex van der Wolk, Hanno Timmer, "European Court of Justice: IP Addresses Are Personal Information," *Westlaw Journal Computer & Internet*, November 4, 2016, <https://media2.mofo.com/documents/161104-wlj-european-court-of-justice.pdf>

¹⁷ Maximiliano D'Auro, Florencia Rosati, Manuela Adrogué and Ambrosio Nougues, "Data protection in Argentina: Overview," *Practical Law*, September 1, 2016, <http://us.practicallaw.com/3-586-5566>

¹⁸ "What an IP Address Can Reveal About You," *Office of the Privacy Commission of Canada*, May 2013, https://www.priv.gc.ca/media/1767/ip_201305_e.pdf

¹⁹ "Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's perspective (2nd Edition)," *Office of the Privacy Commissioner for Personal Data, Hong Kong*, 2010, https://www.pcpd.org.hk/english/resources_centre/publications/books/files/Perspective_2nd.pdf

²⁰ Mangyo Kinoshita, Shino Asayama, Eric Kosinski, "Data protection in Japan: overview," *Practical Law*, November 1, 2014, <http://uk.practicallaw.com/5-520-1289>

²¹ Tom Espiner, "Swiss fileshare software broke DP law, says court," *ZDNet*, September 10, 2010, <http://www.zdnet.com/article/swiss-fileshare-software-broke-dp-law-says-court/>

²² Raphael de Cunto, Julia Arruda, "A civil rights framework for the internet in Brazil," *Financier Worldwide*, July 2014, <https://www.financierworldwide.com/a-civil-rights-framework-for-the-internet-in-brazil/#.WFiuJ7GZMmo>

government agencies have disclosed IP addresses associated with cyber threats through unclassified Joint Indicator Bulletins (JIBs). JIBs have referenced IP addresses and domain names associated with malicious cyber activity to mitigate cyber threats from botnets and Distributed Denial of Service (DDoS) attacks, and have been distributed to U.S. financial institutions and overseas partners through secure channels.²³

Cybercriminals and terrorists may conceal their IP address locations or identities with The Onion Router (Tor), Virtual Private Network (VPN) or proxy tools that enable anonymous web surfing,²⁴ especially with news of criminals getting caught after not using such anonymous web surfing tools.²⁵ With TORWallet, IP addresses are deleted every 30 seconds to anonymize Bitcoin wallet activity.²⁶

New provisions of Rule 41 of the Federal Rules of Criminal Procedure went into effect on December 1, 2016. The Electronic Frontier Foundation asserts in part that Rule 41's new provisions will make it easier for law enforcement to obtain search warrants if a computer uses anonymity-protective software like Tor, a VPN or proxy tools, and urges additional safeguards.²⁷

Online gambling websites, like 10Bet, may address anonymous web surfing directly in their terms and conditions and diverse policies related to privacy,

cookies, fraud, anti-money laundering, and as needed notification to law enforcement and regulatory authorities,²⁸ in part because website users may use such tools to bypass identity verification and geo restrictions.²⁹

Financial crimes investigators may benefit from ExoneraTor, a Tor Project database that allows the public to check whether an IP address was a Tor network relay on a particular day.³⁰

Detecting IP addresses that use VPN or proxy tools is not as easy, although media firms, like Netflix and Hulu, have been blocking users who use VPN or proxy tools to bypass geo restrictions.³¹ Moreover, *Fortune* reported how demand for VPNs has surged recently, given the U.S. Congress' vote to repeal limits on how internet service providers can collect and sell customer data.³²

FinCEN's advisory provides examples of mandatory and voluntary SAR reporting, and encourages the filing of a single SAR to cover interrelated cyber-enabled crimes and cyber-events, like a DDoS cyber-event designed to conceal a cyber-enabled crime that meets the mandatory filing threshold. Basic details on spoofing attacks,³³ for example, should illustrate how criminals launch complex DDoS cyber-events that impersonate users or devices by manipulating IP addresses and other online identifiers, and how financial crimes investigators might describe succinctly such complex cyber-events in SARs.

Other online identifiers

Like IP addresses, online identifiers provided by devices, applications, tools and protocols could be treated as personal data when combined with identifiable data. According to GDPR Recital 30, such online identifiers may include cookie identifiers and radio-frequency identification tags.³⁴

Online identifiers could also include geolocation data, device identifiers like media access control (MAC) addresses, operating system and browser attributes, application data, website activity, and app usage data. Electronic signature authentication forms require detailed attention to device and other online identifiers, as demonstrated by DocuSign's privacy policy.³⁵

As financial services evolve toward greater online and mobile device accessibility, cybercriminals attempt to evade fraud detection by manipulating online identifiers.³⁶

²³ "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015," *The Office of the Director of National Intelligence, The Department of Homeland Security, The Department of Defense, The Department of Justice*, February 16, 2016, [https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_\(103\).pdf](https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf)

²⁴ Mark Wilson, "The best free tools for anonymous browsing 2016," *Techradar*, October 11, 2016, <http://www.techradar.com/news/software/best-free-tools-for-anonymous-browsing-1321833>

²⁵ Catalin Cimpanu, "Crook Who Used His Home IP Address for Banking Fraud Gets 5 Years in Prison," *Bleeping Computer*, December 21, 2016, <https://www.bleepingcomputer.com/news/security/crook-who-used-his-home-ip-address-for-banking-fraud-gets-5-years-in-prison/>

²⁶ "Anonymous Bitcoin Wallet," *TORWallet*, <https://torwallet.com>

²⁷ Jamie Williams, "Expanded Government Hacking Powers Need Accompanying Safeguards," *Electronic Frontier Foundation*, December 14, 2016, <https://www.eff.org/deeplinks/2016/12/expanded-government-hacking-powers-need-accompanying-safeguards>

²⁸ "Terms and Conditions," 10Bet, December 15, 2016, <https://www.10bet.com/help/terms-and-conditions/>

²⁹ "The prevention of money laundering and combating the financing of terrorism - Guidance for remote and non-remote casinos," *Gambling Commission*, July 2016, <http://www.gamblingcommission.gov.uk/PDF/AML/Prevention-of-money-laundering-and-combating-the-financing-of-terrorism.pdf>

³⁰ *ExoneraTor*, <https://exonerator.torproject.org>

³¹ Chris Hoffman, "How to Watch Netflix, Hulu, and More Through a VPN Without Being Blocked," *How-To Geek*, January 20, 2016, <http://www.howtogeek.com/239616/how-to-watch-netflix-hulu-and-more-through-a-vpn-without-being-blocked/>

³² "Congress Voted to Roll Back Internet Privacy Rules. Now People Are Looking to VPNs," *Fortune*, March 28, 2017, <http://fortune.com/2017/03/28/congress-internet-privacy-rules-vpns/>

³³ Neil DuPaul, "Spoofing Attack: IP, DNS & ARP," *Veracode*, <https://www.veracode.com/security/spoofing-attack>

³⁴ "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016," *Official Journal of the European Union*, April 5, 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

³⁵ "Privacy Policy," *DocuSign*, December 15, 2016, <https://www.docusign.com/company/privacy-policy>

³⁶ "Mobile Fraud Gone in a (Device) Flash," *DataVisor*, July 5, 2016, <https://www.datavisor.com/threat-blogs/mobile-fraudsters-gone-in-a-device-flash/>

Money transfer firms, like PayPal, address device and other online identifiers directly in their EU website's terms and conditions. Diverse policies related to privacy, cookies, fraud, anti-money laundering and as needed notification to law enforcement and regulatory authorities are addressed.³⁷

Indicators of Compromise

For at least 10 years, IOCs have been used by computer security firms, like IBM, to refer to cyberattack forensic digital evidence. Such forensic digital evidence may report anomalies, such as IP addresses, domains, files and digital clues that appear to connect the cyber-attacked network with the alleged cyber-attacker,³⁸ with endpoint management tools that may detect security incidents and remediate the environment.³⁹

IOCs may capture unexpected network access details, based on IP addresses associated with certain geolocations.⁴⁰ Cybersecurity firms, like Kaspersky Lab, may publicize IOCs, so that organizations might identify traces of financial cyberattack groups, like Metel, GCMAN and Carbanak 2.0, in their networks.⁴¹

In contrast, over the last few years, the term Indicators of Attack (IoAs) has been used by computer security firms, like IBM,⁴² Intel⁴³ and CrowdStrike, to refer to forensic digital evidence that a cyberattack is occurring or will likely occur in the future, in conjunction with endpoint protection tools that may detect security incidents and remediate the environment.

To CrowdStrike, IOCs reference malware, signatures, exploits, vulnerabilities and IP addresses. IoAs reference code execution, persistence, stealth, command control and lateral movement.⁴⁴


CrowdStrike's presentation on IoAs echoes the Cyber Kill Chain® framework,⁴⁵ which Lockheed Martin, the largest U.S. defense contractor, developed to identify and prevent cyber intrusion activity through seven steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and lateral movement.⁴⁶

The importance of IOCs to the computer security industry is emphasized in a recent assessment about the drawbacks of portraying IoAs as better reporting tools for cyberattack detection and remediation.⁴⁷ Commercial and not-for-profit organizations may reference IoAs more, as they weigh the Cyber Kill Chain®

framework⁴⁸ to deter cyberattacks, including those attributable to nation states.⁴⁹

In conclusion, this timely review of challenges associated with IP addresses, other online identifiers and IOCs should enhance SAR preparation by raising relevant operational issues, such as IPv6 readiness, the proper evaluation and corroboration of IP address data, and the treatment of IP addresses and online identifiers as personal data.

Updates to website privacy notices and terms and conditions may also be timely, along with operationalizing stricter international data protection requirements like the EU's GDPR.

Education may be directed at topics like how cybercriminals attempt to evade fraud detection by manipulating IP addresses and other online identifiers, along with how Tor, VPN and proxy tools have been used to bypass identity verification and geo restrictions. In addition to IOC data, consideration of IoA data may also enhance SAR preparation pursuant to FinCEN's advisory. 

Miguel Alcántar, CAMS-FCI, compliance advisor, Oakland, CA, USA, alcantar@aya.yale.edu

³⁷ "Privacy Policy for PayPal Services," *PayPal*, January 27, 2017, <https://www.paypal.com/uk/webapps/mpp/ua/privacy-full>

³⁸ "Indicators of compromise," *IBM*, 2015, <https://pcatt.org/techblog/wp-content/uploads/2015/10/IndicatorsOfCompromise.pdf>

³⁹ "How BigFix Helps Investigate a Threat in Forensic Activities," *IBM*, https://www.ibm.com/developerworks/community/wikis/form/anonymous/api/wiki/90553c0b-42eb-4df0-9556-d3c2e0ac4c52/page/2a87e237-39ca-4489-81c5-c81124f91a48/attachment/446c7dd5-8737-4342-9acb-3712b0c57556/media/Investigating_threats_with_Bigfix.pdf

⁴⁰ Jason Andress, "Working with Indicators of Compromise," *ISSA Journal*, May 2015, <https://cymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0515.pdf>

⁴¹ "APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks," *Kaspersky Lab*, February 8, 2016, <https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/>

⁴² IBM BigFix Detect, *IBM*, <https://www.ibm.com/us-en/marketplace/bigfix-detect#product-header-top>

⁴³ "Indicators of Attack (IoA)," *Intel*, <http://www.mcafee.com/us/resources/solution-briefs/sb-indicators-of-attack.pdf>

⁴⁴ Jessica DeCianno, "Indicators of Attack versus Indicators of Compromise," *CrowdStrike*, December 9, 2014, <https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/>

⁴⁵ "Cyber Kill Chain®," *Lockheed Martin*, <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>

⁴⁶ Lysa Myers, "Cyber Kill Chain is a Great Idea, But is It Something Your Company Can Implement?," *Infosec Institute*, May 31, 2013, <http://resources.infosecinstitute.com/cyber-kill-chain-is-a-great-idea-but-is-it-something-your-company-can-implement/#gref>

⁴⁷ Dave Dittrich, Katherine Carpenter, "Misunderstanding Indicators of Compromise," *Threatpost Op-Ed*, April 21, 2016, <https://threatpost.com/misunderstanding-indicators-of-compromise/117560/>

⁴⁸ Lysa Myers, "The practicality of the Cyber Kill Chain approach to security," *CSO*, October 4, 2016, <http://www.csoonline.com/article/2134037/strategic-planning-erm/the-practicality-of-the-cyber-kill-chain-approach-to-security.html>

⁴⁹ Dave Dittrich, Katherine Carpenter, "Misuse of Language: 'Cyber'; When War is Not a War, and a Weapon is Not a Weapon," *Threatpost Op-Ed*, August 9, 2016, <https://threatpost.com/misuse-of-language-cyber-when-war-is-not-a-war-and-a-weapon-is-not-a-weapon/119740/>

CYBERSECURITY AND BSA/AML

In October 2016, the Financial Crimes Enforcement Network (FinCEN) published an advisory document with frequently asked questions concerning cyber-events and cyber-enabled crime to financial institutions.

When filing suspicious activity reports (SAR) it is important for financial institutions to review this FinCEN guidance, in order to receive key information as to what to include on the SAR. Some examples of the information are noted in the excerpt below:¹

Source and destination information:

- IP address and port information with respective date timestamps in UTC
- Uniform Resource Locator (URL) addresses
- Known attack vectors
- Command and control nodes

File information:

- Filenames of files suspected to be infected with malware
- MD5, SHA-1, or SHA-256 hash information
- Email content

Subject user names:

- Email addresses related to suspicious activities

- Social media accounts/screen names related to suspicious activities

System modifications:

- System registry modifications
- Indicators of system compromise
- Common vulnerabilities and exposures

Involved account information:

- Potentially or actually affected account information
- Potentially or actually involved virtual currency accounts (case sensitive)

As a Bank Secrecy Act/anti-money laundering (BSA/AML) officer, venturing into the cybersecurity realm is often new or unfamiliar territory. Although the industry trend is that it is becoming increasingly necessary for BSA/AML officers to learn and understand more about technology and cyber threats, it is essential, given the guidance from October, to establish regular meetings between the BSA/AML team and the institution's information security team.

Communication within the financial institution is key. It is also important that the BSA/AML team reviews the bank's incident response plan addressing cyber-events and cyber-enabled crimes in order to establish the BSA/AML team's role within the event handling process. Including the BSA/AML team enables all cyber-events to be properly reviewed for possible SAR filing. Tracking and reviewing cyber cases is important to identify common patterns and emerging trends related to suspicious activities. Understanding key similarities in those cases can be facilitated by leveraging case data analytics and aggregation tools. Providing this enhanced analysis and reporting to law enforcement can assist them in developing their cases and put the key pieces of a very complex puzzle together. Throughout the case your FI team would more than likely be working with law enforcement, so it is important to document at what point in the process would the bank file a SAR. Would it occur at the end of the investigation so

¹ "Frequently Asked Questions (FAQs) Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime and Cyber-Related Information through Suspicious Activity Reports (SARs)," FinCEN, October 2016, <https://www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-events-cyber-enabled-crime-and-cyber>




that you can ensure that all of the information is gathered and organized? Or would it possibly be within 60 days of detecting the cyber-event? Also, what would your FI consider to be a reportable cyber-event? Would it be only if there is a loss to customers or the FI or if the cyber-event had a significant customer impact? Per the FinCEN guidance: "In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions of attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event."

These are all items that should be discussed within the BSA/AML team and information security team to determine what your institution's policy will be going forward. In making those decisions it is essential to document what decisions are made and who in the FI is responsible for what part.

When working through a case, try to gather as much information as possible from your information security team and from customers that may have been victims of a cyberattack. It is also advantageous to create a case collection form for collecting information specifically about cyber-events, in order to guide the information security team to capture the specific related information needed to complete the SAR reports. Obtaining as much information as possible enables the bank to effectively assist law enforcement in developing and pursuing their cases and identifying emerging industry trends.

Along with the cyber incident response plan, it is also important to create BSA/AML and fraud incident response plans for the separate business lines within the institution. These plans should complement each other and align upward to an enterprise-risk event and incident response plan that can better align with the institution's business continuity plans.

The BSA/AML incident response plan should account for the BSA/AML team's role in addressing and documenting cyber and other high-risk events and incidents potentially resulting in regulatory action or monetary penalties.

In conclusion, it is important for all BSA/AML officers to review FinCEN's advisory and to work with the institution's information security team to develop effective plans for addressing and reporting on potentially adverse cyber-events. An effective program identifies, gathers and documents as much related information as possible for cyber-events that may occur at your institution. Finally, sharing this information with law enforcement, so that it may be used to more effectively develop their cases and identify industry trends, is partnership at its finest. 

Joe Soniat, CAMS-FCI, vice president and BSA/AML officer, Union Bank and Trust, Glen Allen, VA, USA, robert.soniat@bankatunion.com

THE SUCCESS OF PUBLIC-PRIVATE PARTNERSHIPS



In August 2015, the St. Paul Police Department launched the Criminal Proceeds Unit. The unit is dedicated to the investigation of money earned from criminal activity, be it the sale of narcotics, human trafficking, fraud or other felony level crimes. Money is the lifeblood of a criminal organization and criminals are often motivated by easy profit and do not fear incarceration. Valuable pieces of evidence can be found by examining the movement of money obtained from criminal activity. With this new direction, the Criminal Proceeds Unit has significantly impacted the St. Paul Police Department and the community it serves. Every day, investigators work on cases and “follow the money.”

Demand for the services of the Criminal Proceeds Unit has quickly grown beyond narcotics and human trafficking to include investigations in elder abuse, theft, fraud and tax evasion. The tools and techniques developed by the Criminal Proceeds Unit have enhanced the St. Paul Police Department's ability to investigate crime along with taking a proactive approach to financial investigations. But our success does not happen alone. Like all organizations, the St. Paul Police Department depends and benefits from its many partnerships with both the private sector and other government agencies. Some of our success has come from being task force officers with the U.S. Secret Service, members of the Minnesota Financial Crimes Task Force and serving on the Minnesota Suspicious Activity Review (SAR) team. The St. Paul Police Department's Criminal Proceeds Unit works extensively with the local banking community by conducting training and networking with bank investigators.

The Criminal Proceeds Unit is also active with the local ACAMS Greater Twin Cities (GTC) Chapter. The ACAMS GTC Chapter has greatly accepted the participation of law enforcement within their chapter and has even asked a member of the Criminal Proceeds Unit to serve on their board. This partnership has benefited the ACAMS GTC Chapter and the St. Paul Police Department by deepening our working relationship and educating one another. Shannon Bennett, GTC chair of the board, stated, “We feel very fortunate to have law enforcement serve as members on the board. We find their contributions and insight has been instrumental in our success, which includes providing ideas for topics and speakers that truly add value to the mission of the chapter to provide education related to financial crime to our community.”

The success of partnering with private and public sector institutions has resulted in a series of successful cases and prosecutions of criminals who typically might be too hard to catch at the local level and too elusive for over-worked federal law enforcement agencies to catch. The first success was in the investigation of Papa Dmitri's Pizza. For many years, law enforcement heard that Papa Dmitri's was a front business for a criminal enterprise run by a longtime St. Paul gang member. By focusing on the financial activity of Papa Dmitri's Pizza, investigators were able to arrest the owners of the pizza shop along with obtaining a conviction of federal weapons charges along with concealing criminal proceeds through a business. This was the first time this statute was successfully prosecuted in Ramsey County, St. Paul, Minnesota.

Next, the Criminal Proceeds Unit was brought in to assist on a large embezzlement scheme of a local business in St. Paul. An employee who worked in the payroll unit of a large company in St. Paul managed to embezzle \$450,000 by masking payments to her in the names of other employees. To make matters worse, when confronted, the suspect tried to convince investigators that her boyfriend, who she claimed committed suicide, wrote a suicide note claiming responsibility for her crime. Not only was the boyfriend alive and well in western Wisconsin, but the suspect managed to use the embezzled funds to purchase many expensive assets, such as two new vehicles and a semi-truck. Working with private partners and the U.S. Secret Service, these assets were recovered, the suspect went to prison and money from the sale of the recovered assets was returned to the victimized company to lessen the total loss.

Perhaps the biggest case, and certainly the most interesting case the St. Paul Police Department's Criminal Proceeds Unit investigated was the Seng Xiong, "Hmong Tebchaws," affinity fraud scheme. This case was worked with the cooperation of the U.S. Secret Service and the Federal Bureau of Investigation (FBI). Tipped off by a private sector financial partner, St. Paul investigators began to track the financial activity of the suspect, Seng Xiong. What investigators quickly learned was that Xiong had not only manipulated people, but was also victimizing a vulnerable population. Xiong promised his victims a new country and financial security. His scheme was successful as it tapped into many deeply held dreams by the Hmong community of one day having a country of their own.

Xiong was a drifter; a man with no means of support other than the lies he spewed about his top secret work with the U.N. and the White House, which he said supported the establishment of a country for the Hmong people. The Hmong people are refugees from the northern highlands of Laos. A nomadic group who never had their own country, but fought alongside U.S. troops during the "Secret War" against communist soldiers in Vietnam. Fiercely loyal to the

U.S. government, many Hmong people believed they were owed their own country and that secret deals and back-room meetings with intelligence officials is how a new country would come about. Xiong, "talked the talk" and convinced a population eager to hear a certain message that he was just the person to pull it off.

The Hmong were persecuted for their allegiance to the U.S. They fled Laos into camps in Thailand and hundreds of thousands of Hmong people started to migrate from Southeast Asia to the U.S., Australia and France. Assimilation was tough and many of the older generations longed to return to the hills of Laos and have their own piece of land. In this narrative, Xiong saw an opportunity. Orchestrated from Minnesota and California, through a network of conference call lines and YouTube videos, Xiong convinced the poor and disenfranchised that he was in the middle of holding high level meetings with the U.S. government and they had "authorized," a new Hmong country. For a small investment, Xiong told his eager audience that their "dreams would become a reality."

Xiong enticed "investors" with promises of 10 acres of land, a five-bedroom house, free education for your children, free healthcare and good paying government jobs. Depending on your investment level of \$3,000, \$4,000 or \$5,000, you would see a yearly return on your investment based on the revenue the government collected. As a "founder" of the new country, your name would be etched in the halls of time. The scheme worked as Xiong managed to raise over a million dollars from victims in 17 states, Australia and France. Hmong people, eager to return home to reclaim the lands of their ancestors, lined up to wire him money or went to their local bank to make a direct deposit into Xiong's personal checking account.

When Xiong realized the government was onto his scam, he tried to flee the country from Los Angeles International Airport. Investigators from the Criminal Proceeds Unit, along with the Los Angeles FBI and the U.S. Secret Service arrested Xiong as he tried to board an airline destined for Thailand. In the end,

investigators seized \$1.7 million in cash held in multiple accounts under Xiong's name. At trial, Xiong pitched a far-fetched story to the jury about funding insurgencies and fighting the communists in Southeast Asia, but they did not buy it. Xiong was convicted in federal court for mail and wire fraud.

Successes like these are not built overnight and they are not the work of any one person. The success of the St. Paul Police Department's Criminal Proceeds Unit depends largely on the partnerships established with our banking community and local and federal law enforcement. The Criminal Proceeds Unit actively participates in many ACAMS events, attends the annual conferences and continues to pursue strong working relationships with all our partners. Working with ACAMS has provided invaluable tools and networking opportunities for the unit. In fact, members of our team always leave each training session with an idea on how better to serve the citizens of St. Paul and the community that surrounds us.

At local ACAMS events, the Criminal Proceeds Unit meets and speaks with bankers and other professionals in the financial sector to discuss recent human trafficking cases, narcotics, terrorism and the latest trends in fraud. Although still a very new unit with much to learn, the Criminal Proceeds Unit is poised to help the St. Paul Police Department accomplish its mission of serving the citizens of our city by tackling those tough to catch criminals who exploit the financial system for their own selfish gain. This cannot be done alone. Members of the Criminal Proceeds Unit are eager to continue their participation with ACAMS. Through networking, partnerships, knowledge sharing and mutual assistance, the St. Paul Police Criminal Proceeds Unit, along with its many wonderful partnerships, is building a stronger police department and a safer community. **A**

*Daniel Michener, investigator, St. Paul Police, St. Paul, MN, USA,
daniel.michener@ci.stpaul.mn.us*



ADVANCING AML PROGRAMS WHILE ADOPTING NEW TECHNOLOGY

As leaders in the anti-money laundering (AML) field, every day we are tasked with protecting our customers and our businesses against increasingly frequent and sophisticated threats from bad actors.

As we look ahead, rapidly evolving technology may provide the single greatest opportunity for advancing progressive AML programs in history. Whether augmenting investigative processes with big and fast data, or harnessing the power of machine learning or robot process automation to identify threats, the opportunities can feel endless—and daunting.

For example, traditionally, AML shops have relied on third-party software platforms that are regularly updated. After the initial launch, training was minimal only on the updated features. Now, that landscape is starting to rapidly change. AML organizations are either creating their own software systems that are updated much more frequently or leveraging multiple third-party platforms (all of which update more frequently to keep up and demand much more investigator training time). These changes are starting to fundamentally affect how an investigator spends his/her time, shifting it to potentially different skillsets needed to digest the information. While all of this is good, it is very disruptive to the average person trying to keep up with the change.

Another example is a concern of information overload. The ability to harness much more data through software is exploding, so the investigator is increasingly seeing more and more data with potential associated complexity. However, this can also lead to “analysis paralysis” where the investigator can get stuck wading through all of the information that takes a lot more time and may not improve the investigation. With the pace of software change and the explosion of data, the average investigator is being inundated with change.

As a result, managers can be left balancing the tension between meeting the practical daily challenges of our industry and the need to transform how his/her team works by implementing the latest technology—all while keeping employees engaged, happy and productive.

Leading the transformation

During this time of change, how can managers simultaneously drive organizations forward without leaving their teams behind? The answer may be to take a page out of the digital developer's playbook and adopt more agile and innovative operating principles.

There are six fundamental management principles that can serve as enablers to meeting these challenges. These core elements include:

1. *Work in short cycles:* Have you ever heard the joke, "How do you eat an elephant?" The answer is "one bite at a time," and that principle holds here. When adopting new technology, take small steps. Try something new and see how it works. If it fails, you have invested very little. If it succeeds, improve on it.

Try working in two or three-week increments called "sprints." Teams set very specific goals for this period and fully focus all efforts on executing them. At the end, they demonstrate tangible accomplishments to ensure they are on the right track.

Sprints limit an issue called "feature decay." In many cases teams are provided holistic project requirements that require months of work. By the time the product is delivered, the customer's needs often change. Working in short cycles can help avoid this trap.

2. *Empower your team:* First and foremost, give your team input over the work they do and fully staff them so that they are able to get their work done with as few outside needs as possible. For example, if you have software development teams, each team should have a developer, a tester, a product owner (representing the customer) and anyone else directly required to complete the task. The goal is to reduce dependency on any outside resources.

Second, hold planning sessions every three months to map out the next quarter's work. Overall guidelines and strategy are set by the executive management and the teams then self-determine what they can accomplish and how they will be measured. At the end of the planning cycle, each team member "votes" on a scale of one to five, with five being confident that the work can be done. Any votes of three or below are addressed before the planning is considered complete. Allowing team members to have direct input and control over their work product leads to increased associate satisfaction and throughput.

3. *Check-in frequently:* A key element of increasing efficiency is in effectively managing meetings. The time invested in checking schedules, setting a time, an agenda and preparing materials is a large driver of inefficiency. So, how do you avoid this trap?

Try using a series of regular, short (generally 15-30 min.) scheduled program team meetings called "stand-ups" or "huddles." No materials should be prepared. It should just be a simple check-in as to what was accomplished yesterday, what is to be completed today and if there are areas where help is required. A similar meeting series should be held through the head of the department, in order to provide an opportunity for leadership to gain transparency into work progression and directly remove roadblocks that the team may be facing.

4. *Be retrospective:* The only way to know how to improve is to regularly review how you have performed; however, this step is often skipped in favor of the next priority. Hosting a regular cadence of reviews reaps great benefits. At the end of each cycle (I recommend at least monthly), review what went well, what did not and vow to improve one or two key things.



A key element of increasing efficiency is in effectively managing meetings

5. *The customer is everything:* If you are struggling to align as a team, focus on the customer or program value. How do we know we are shipping something that will truly make an impact? How do we find out? How does that affect what we prioritize? These are fundamental questions to regularly ask.
6. *Practice servant leadership:* If there is one key to making these principles work, it is evolving to a servant leadership model. "Servant leadership is a very popular leadership model that was developed by Robert K. Greenleaf in 1970. The short definition is a servant leader serves the people he/she leads, which implies that employees are an end in themselves rather than a means to an organizational purpose or bottom line."¹ In this model, leaders prioritize the needs of others first by empowering individuals to grow and perform at a high-level. It sounds simple, but this is no small effort. Traditional management techniques can emphasize a very different style, so coaching leaders to embrace this new approach can be a challenge that should not be underestimated. The following are key elements of servant leadership:

¹ Mitch McCrimmon, "Servant Leadership," Leadersdirect, <http://www.leadersdirect.com/servant-leadership>

- *Go and see*: Most management models are centered around the employees going to the leader. In this style, the leader must get out and visit the teams, regularly walking the floors and talking to their teams to understand progress and where there are obstacles that can be cleared.
 - Listen*: Servant leadership emphasizes “active listening” with employees. This means leaders must avoid the urge to immediately attempt to problem solve and instead take time to truly understand the challenge. It is important to avoid the “Why” word that can cause defensiveness, and instead ask questions starting with “When,” “How,” “Who,” etc., to get to the crux of the obstacle. This an important skill that must be developed.
 - Focus on the future*: There are three “domains” of conversations—past, present and future. Most conversations are in the “past” (e.g., what happened,

why it did not work, etc.). Next time you are in a meeting, try the following exercise: Make a mark every time someone talks about the past, the present and the future. You will most likely find the majority of conversations focus on the past, bogging down on what went wrong and why it happened, instead of focusing on future improvements.

A skilled servant leader can help move the conversation to the present and then to the future. This allows the group to break out of a rear-facing focus and instead identify what could be and how to get there. The table below provides an example of this.

Now obviously, conversations are not quite so quick and stark. However, the point is that being a servant leader is a lot like being a coach. Your job is to help the whole team move forward.

Traditional Management Conversation	Servant Leader Conversation
Boss: OK, how do we fix the fact that we are four days behind?	Boss: OK, let's talk a bit about the production issues, what are your thoughts?
Person A: It is a huge problem, been building for a while.	Person A: It is a huge problem, been building for a while.
Person B: Well, you are right, I kept telling everyone that this would happen.	Person B: Well, you are right, I kept telling everyone that this would happen.
Person A: Well, I never heard it from you and if you had said something we wouldn't be in this situation.	Boss: Yep, in the last retrospective, I remember this issue was discussed. What if we can cut back on all meetings for two weeks? This would help production, wouldn't it?
Boss: Guys, I don't have time for this, this has to get fixed...	Person A: Well, it could, but we will never do this. Meetings take up half our days.
[Conversation spirals]	Boss: We do have a ton of meetings. What would have to happen to reduce them?
	Person B: We could first focus on what are the “nice to have” meetings versus the “critical” ones and then....
	[Conversation moves to specific steps that can be taken]

Final notes

Working smarter by keeping your customer in mind, working in shorter cycles and building an empowered team can reap benefits to meet the consistently high demands of an ever-evolving industry.

As you start this journey, remember these are universal techniques that can be applied in every type of group such as investigations, transaction monitoring, processes and development or support of software. As threats continue to grow, leveraging these techniques can improve your overall ability to execute your mission. 

*Brad Dolbec, CAMS, senior director of AML, Capital One, Richmond, VA, USA,
brad.dolbec@capitalone.com*



Improve AML compliance and lower costs.

Resolve entities with superior accuracy and precision

Your ability to manage the cost of compliance and regulatory risk hinges on a highly accurate single view of the customer. This level of entity resolution for AML is available from Pitney Bowes. Every day, we help financial institutions find, link and visualise relationships, all in the effort to reveal the comprehensive view they need to succeed.

Overcome data limitations to uncover suspicious activity with greater speed and precision.

Learn more at pitneybowes.com/sg/aml



“IT’S NOW POSSIBLE FOR A DRUG DEALER TO SERVE TIME IN A FORFEITURE-FINANCED PRISON AFTER BEING ARRESTED BY AGENTS DRIVING A FORFEITURE-PROVIDED AUTOMOBILE WHILE WORKING IN A FORFEITURE-FUNDED STING OPERATION.”

—ATTORNEY GENERAL RICHARD THORNBURGH, 1989¹

When dealing with predicate offenses, it is difficult for a financial institution to think about collaborating with the several law enforcement agencies (local and international) immersed in this process without having a strong culture of compliance in place that directly or indirectly ensures an efficient methodology that clearly identifies the ultimate beneficial owners of the entity whose assets are trying to be confiscated.

When looking for a confiscation or forfeiture order, only a sound and forceful Customer Identification Program (CIP) built within the appropriate anti-money laundering (AML) and internal controls will guarantee the identification of all relevant beneficial owners spotted with a compelling know your customer (KYC) program.

The prior examples support the importance of building, maintaining and promoting a culture of compliance that not only satisfies regulatory requirements, but also assists law enforcement agencies when trying to prosecute and punish all who use the financial system for the purposes of laundering illicit funds.

Defining compliance within the AML spectrum

According to Martin T. Biegelman, managing director of regulatory, forensics and compliance for Deloitte, “Compliance means following the law and more. It’s making sure organizations adhere to all applicable legal requirements. It is a detailed and complex process.”² Now, let us convey this basic concept into AML context where financial institutions have to deal with more and more stringent regulations and aggressive domestic and international law enforcement requirements. Compliance would be the process aimed at assuring that all the Bank Secrecy Act (BSA) and Office of Foreign Assets Control (OFAC) reporting, filing and record keeping requirements are met accordingly.

Current AML compliance programs must be able to include practical ways (e.g., designing a robust BSA and terrorist financing risk-based process and procedures around Section 314(a) of the USA PATRIOT Act) to aid law enforcement bodies to discover proceeds from crime, including terrorist financing. The only way to efficiently do this is by creating and fostering a culture of compliance that not only relies on its three conventional catalysts (training, internal control and internal audit), but also on an appropriate and adequate set of core values (where ethics play a factual and critical role), effective communication channels, sound governance and proactive leadership.

Core values

A financial institution’s core values should be founded on bulletproof ethics and principles that intrinsically assure all the processes considered in its AML compliance program are carried out by managers and employees that vehemently believe that what they are doing is best for their organization and for society in general. No matter how complex, well-structured and inclusive this

program is, if the entity’s core values do not transpire in the minds of every AML compliance process stakeholder, it will be hard to optimally attain the desired final purpose of the program.

For instance, if a new client onboarding’s analyst (despite having a strong set of CIP and KYC procedures or not), does not apply strong ethics and integrity principles toward further strengthening the financial institution’s corporate compliance, firmly believing that it is the only way to strongly combat any possible money laundering attempts, then an accurate identification of beneficial owners will be nearly impossible.

Law enforcement agencies will rely strongly on due diligence and enhanced due diligence practices when inquiring for “obscure” ownerships, especially for the ones that involve complex business structures.

As a matter of fact, during the last G20 summit carried out on July 2016 in Hangzhou, China, the Financial Action Task Force highlighted the urgency to implement major improvements in some countries where the beneficial owner problem was assessed.³

A clear example of how imperative it is to know the true identity of the financial institution’s customers along the CIP process, is, without a doubt, the final rule issued by the Financial Crimes Enforcement Network, which pertains to straightforward customer due diligence requirements aimed to identify and verify the identity of beneficial owners of legal entity customers subject to certain exclusions and exemptions. The rule highlights, among other aspects, the importance of: “1) Enhancing the availability to law enforcement, as well as to the federal functional regulators and self-regulatory organizations (SROs), of beneficial ownership information about legal entity customers obtained by U.S. financial institutions, which assists law enforcement in financial investigations and a variety of

regulatory examinations and investigations and 2) Increasing the ability of financial institutions, law enforcement and the intelligence community to identify the assets and accounts of terrorist organizations, corrupt actors, money launderers, drug kingpins, proliferators of weapons of mass destruction and other national security threats, which strengthens compliance with sanctions programs designed to undercut financing and support for such persons.”⁴

Effective communication

Effective communication is another critical element to consider when trying to foment a vigorous culture of compliance. For example, values need to be communicated in a convincing fashion from the top.

Also, due to the regulatory nature of the AML sector, communication systems, protocols and processes need to work in an extremely synchronized manner, always avoiding procedural and/or systematical communication breaches.

Understanding and acknowledging the different AML laws and regulations are the first priority. Entities functioning under the BSA, USA PATRIOT Act and OFAC must implement, adjust, manage and monitor their communication channels and frameworks in order to void any possibility of falling into a “willful blindness” situation that might be created by communication-related gaps or breaches. In fact, neither the entity itself, nor its employees, should be able to evade a criminal accusation or civil indictment by alleging that they did not know certain AML statutes were being infringed.⁵

A great scenario to describe the importance of having an effective communication system in place is when dealing with 314(a) requests. A 314(a) request is a powerful mechanism used by different law enforcement agencies in order to identify bank and other financial

¹ Sarah Stillman, “Taken,” *The New Yorker*, August 12, 2013, <http://www.newyorker.com/magazine/2013/08/12/taken>

² Martin T. Biegelman, *Building a World-Class Compliance Program: Best Practices and Strategies for Success*, published by Wiley, Hoboken, New Jersey, p. 2.

³ “FATF Report to the G20: Beneficial Ownership,” FATF, September 2015, <http://www.fatf-gafi.org/media/fatf/documents/reports/G20-Beneficial-Ownership-Sept-2016.pdf>

⁴ “Customer Due Diligence Requirements for Financial Institutions,” FinCEN, July 11, 2016, <https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions>

⁵ Martin T. Biegelman, *Building a World-Class Compliance Program: Best Practices and Strategies for Success*, published by Wiley, Hoboken, New Jersey, p. 2.

institution accounts that might be associated to the targets of a particular investigation.⁶

Due to its complexity, this process demands from financial institutions, a competitive, efficacious and highly restricted communication network, structure and procedures that soundly and timely address law enforcement requirements in order to guarantee the feasibility and integrity of the investigation.

Sound governance

The term governance is defined by Richard M. Steinberg (in his book *Governance, Risk Management and Compliance: It Can't Happen to Us—Avoiding Corporate Disaster While Driving Success*), as “the allocation of power among the board, management and shareholders.” Steinberg adds that nowadays the concept goes beyond the firm's board of directors' scope and incorporates stakeholders that are identified all the way down from senior levels to the management ranks.

With Steinberg's point in mind, it is critical to highlight the significance of the AML risk management committees, usually led by independent directors, chief compliance officers (CCOs) and chief risk officers (CROs), among other key AML stakeholders.

These committees are meant to recognize and detect all of the AML risks a financial institution could be facing. One of the key functions of an AML risk management committee is to assess the AML risks and elaborate a plan in order to manage and monitor these risks. This strategy may include de-risking, adjusting operations to lessen risks, etc.

When facing potential suspicious activity report filings and/or 314(a) and 314(b) requirements and inquiries issued by law enforcement agencies, a solid and preemptive governance

structure is crucial, as well as the involvement of both the board and of course management.

Proactive leadership

Undoubtedly, the best persons to encourage employees to embrace a culture of compliance are the chief executive officers, directors, CCRs and CCOs. They are required to lead by example and by communicating the organization's core values with passion and assertiveness. Leaders at a financial institution are the ones chosen to answer the call of action. In addition, leaders can set the tone at the top for the compliance process.

Positive and authentic leaders know how to inspire others along the organization in order to comply with relevant policies, laws, regulations and with the different inquiries and investigation mandates that come from law enforcement agencies across the globe.

Conclusion

Preventive, detective and corrective AML measures are attributes of a trend that indicate financial institutions and gatekeepers are expected to exercise a police-like function from the regulators and law enforcement agencies. The privatization of law enforcement is a reality and today in many jurisdictions law enforcement is asking the private sector for more participation. For instance, a European Parliament and Council Directive now enforces an obligation on accountants to report irregularities.⁷

Also, according to FinCEN, inadequacies have been identified in recent AML enforcement actions, which confirms that the culture of an organization is decisive to its compliance.⁸

It is important to note that the U.S. financial intelligence unit highlights how critical it will be for banks and financial institutions affected by trends (i.e., those

Leaders can set the tone at the top for the compliance process

AML compliance-related deficiencies closely associated to organizational culture matters) to build a culture of compliance founded on a genuine and strong leadership of engagement, robust communication methodologies, forceful core values, as well as proactive governance. In fact, FinCEN states that having a strong culture of compliance will help to identify significant relationships, trends and patterns. For example, BSA reports unveil the relationships between illicit actors and their financing networks, empowering law enforcement to identify the primary behavior of concern and to utilize forfeiture and sanctions to disrupt their capacity to operate and finance their unlawful behavior. BSA reports also reveal trends and patterns on criminal, terrorist and other evolving threats that enable law enforcement to optimize their scarce resources by remaining focused on key information and data sometimes provided by financial institutions.

Thus, the transparency, effectiveness and timeliness used by financial institutions to manage, report and respond to AML and terrorist financing-related matters brought by law enforcement agencies, are the greatest elements in delivering the most significant information available to law enforcement and others protecting the U.S. and constitutes a unique tool that is useful when pursuing and confiscating the proceeds of crime. **FA**

Jaime A. Verástegui, CAMS-Audit, CFE, AML QA manager, Santander Private Banking, Miami, FL, USA, jverastegui@bpi-gruposantander.com

⁶ FinCEN's regulations under Section 314(a) enable federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 39,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering (<https://www.fincen.gov/sites/default/files/shared/314factsheet.pdf>).

⁷ Guy Stessens, *Money Laundering: A New International Law Enforcement Model*, Cambridge University Press, p. 179.

⁸ “Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance,” FinCEN, August 11, 2014, <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a007>

UNLOCK YOUR GUIDE TO AML



Given the increasing regulatory scrutiny related to AML issues and complex challenges, financial services companies are realising the importance of implementing and maintaining a robust AML program.

Protiviti's guide to US Anti-Money Laundering Requirements begins by summarising the basic principles of money laundering and terrorist financing. The guide also delves into many of the practical considerations of maintaining effective AML/CFT Compliance Programs, such as Risk Assessments, Know Your Customer, and Transaction Monitoring and Investigations, including the selection and use of enabling technology.

Get the guide at **[Protiviti.com/AML](https://www.protiviti.com/AML)**

[protiviti.co.uk](https://www.protiviti.co.uk)

protiviti[®]
Face the Future with Confidence

THE BLOCKTRAIN has left the station

One of the days when a mysterious internet-based currency called bitcoin was seen simply as a tool used by criminals to purchase illicit goods and launder money. Today, Bitcoin is recognized as a promising innovation and its underlying technology (blockchain) has inspired the design of a multitude of new blockchains that work in nuanced ways to accomplish a multitude of tasks. Successful blockchain-related businesses are blooming across the globe and financial institutions, law enforcement and governments have taken notice. The new discussion is not about whether blockchains are here to stay, the discussion is about the many ways blockchains can be leveraged to create revolutionary new applications and replace antiquated systems. The most prevalent blockchain application to date remains the transfer of value through cryptocurrencies, and it is imperative that anti-money laundering (AML) professionals understand, and keep up-to-date with this technology and the related money

laundering risks and solutions. This is particularly true as cryptocurrency valuations have soared as much as 300 percent in recent months, attracting the attention of investors (and possibly criminals) worldwide. This article highlights two events organized by ACAMS chapters in February, which introduced AML professionals to the world of blockchain with a purpose of fostering a culture of learning and collaboration.

The Chicago and Toronto ACAMS chapters hosted an event in their downtown cores, where they highlighted the universe of blockchain applications and their accompanying compliance issues and solutions. The events' participants were an eclectic group that included financial institutions, government officials, central bankers, Fintech startups, public-private alliances, and compliance and analysis companies. The wide range of professionals who are involved in this space highlights the breadth, sophistication and interest this

technology has roused, and signals the staying power of this technology. As AML professional Peter Warrack noted in the Toronto event, "The Blocktrain has left the station and it's time to get onboard."

The network of blockchain experts assembled at these events was like a microcosm of the industry. It highlighted how businesses, law enforcement, compliance professionals and governments are working toward the same goal: using blockchain technology to innovate while still safeguarding society.

Learning about blockchain technology

In both cities, the audience received 'Blockchain 101' lessons that summarized how the technology works and the various benefits offered. Generally, blockchains are a type of distributed ledger that serves as an incorruptible record of transfers of ownership.



Perhaps the best way to introduce an audience to blockchain technology is by showing them a live example of how transactions work and this is exactly what Jonathan Solomon, co-founder and CEO of Digital Mint and Joe Ciccolo, founder of BitAML, did in Chicago. By presenting the process of transferring cryptocurrencies through exchanges, it is easier to introduce concepts like wallet ownership and how wallets are generated. Generally, cryptocurrency exchanges create wallets for clients free of charge. Providing wallets is comparable to providing email addresses. A person can have multiple email addresses, email addresses are always unique, and anyone who knows the login information can use them. However, describing the multiple differences and subtleties of the various popular

blockchains necessitates much more time and research than a single article can accommodate.

Blockchain-based business

While the best-known blockchain-related businesses are exchanges, entrepreneurs have found many other uses for blockchains. Businesses can provide notary-like services, such as time stamping documents¹ or track diamonds from the mine to the consumer and beyond.² For example, Joseph Weinberg, CEO of the Canadian-based money services business (MSB), Paycase, explained how his company makes use of blockchain technology in order to send remittances internationally.

The company offers clients a computer and mobile-based platform that

provides a relatively cheap alternative to legacy systems such as wires. The service is fast (sometimes instant) and offers bank-to-bank transfers, cash-pick up and even door-to-door cash delivery. In addition, it allows money to be sent to unbanked areas in the world where few options are available, despite the dire need for financial assistance.

Cryptocurrency transaction monitoring and compliance

This Canadian-based MSB uses blockchain infrastructures to move value across borders, using banks and partners in the beneficiaries' jurisdiction to get money to its final destination. This business model is different from cryptocurrency exchanges, which are the most popular value transfer mechanism for

¹ <https://bitproof.io/>

² Luke Parker, "Ten Companies Using the Blockchain for Non-Financial Innovation," Brave NewCoin, December 20, 2015, <https://bravenewcoin.com/news/ten-companies-using-the-blockchain-for-non-financial-innovation/>

cryptocurrencies. The main difference between the two is that cryptocurrency exchanges provide clients with cryptocurrency wallets. People can use these wallets to exchange fiat currency into cryptocurrency and use said cryptocurrency to speculate on cryptocurrency value, transfer wealth and purchase goods and services worldwide. Retailers who accept cryptocurrencies, usually bitcoin, range from small shops to Amazon.com.

Wallets can provide a certain amount of anonymity for the wallet owners, and this was once amongst the greatest hurdles exchanges had to get over: how to mitigate criminal use of cryptocurrencies. Ciccolo and Solomon explained that what was once seen as a hurdle has turned out to be a gift to AML investigators. Although it is true that the owners of cryptocurrency wallets are not publicly known, many blockchains offer a complete public record of all transactions that have ever occurred and this information can be leveraged for investigative purposes. In the Chicago event, several free tools were used to trace bitcoin transfers including blockchain.info.com, a free online wallet and a blockchain explorer service. Free tools that share massive amounts of information gave Ciccolo a good reason to call blockchains “314(b) on steroids.”³

As exchanges have evolved, so have companies that provide know your customer (KYC) enhanced due diligence and transaction monitoring services. One such company is Chainalysis—their CRO, Jonathan Levin, joined the Toronto event. Levin explained how the Bitcoin blockchain can be leveraged to risk score and track wallet activity within this publicly broadcasted blockchain. Chainalysis has created algorithms that detect and track activity through scenario-based monitoring and alerts, which can trigger on a multitude of predetermined suspicious and unusual schema. The software is visually intuitive and provides the end user with the ability to find connections and track transactional history quickly

and easily. Such software gives exchanges some of the tools necessary to conduct AML investigations. It also gives exchanges the ability to present data from an independent source that verifies their client's activity. Such reports can be useful in growing or improving relationships with financial institutions, regulators and law enforcement.

In addition, new blockchains have emerged such as ZeroCash, which allow users to transact through payments that reveal neither the origin, destination, or amount of the payment. Because such cryptocurrencies do not provide a public history of transfers, new hurdles dealing with lack of transparency have emerged. That said, the volume of Zcash transferred every day is a fraction of better-known cryptocurrencies, such as bitcoin (~\$11.4 million daily vs ~\$1 billion daily).⁴ The low volume suggests there are much fewer Zcash users, in comparison to other cryptocurrencies. The high volume of Bitcoin users suggests that users are willing to give up a certain amount of privacy for the ease of use.

Compliance solutions by companies like Chainalysis are necessary for sustainable growth of cryptocurrencies, as they allow responsible companies to combat the use of cryptocurrencies for nefarious activities. Such companies are looking to create future solutions to blockchain risks and are already helping to combat existing crimes. One such crime that has been linked to the use of bitcoin is human trafficking.

Combating human trafficking

Warrack, from the Bank of Montreal, presented in Toronto on the connection between bitcoin and human trafficking.

Some online classified ad platforms have garnered a seemingly endless stream of adverse media, and government and social pressure due to their reputation as facilitators of the online sex trade. While prostitution may be



legal in various jurisdictions, human trafficking (coercing a person through threats and violence to perform sexual acts for money) is not, and the illicit profits generated through this crime are often laundered. In recent years, major credit card companies have stopped supporting payments to such platforms, and since then, bitcoin has become the primary method for sending payments to such companies.

Law enforcement and entities that are expected to report instances of money laundering associated with human trafficking should become acquainted with the different ways Bitcoin is used to purchase ads on adult classified ad platforms. While most Bitcoin exchanges have KYC regimes that human traffickers would want to avoid, there are payment methods available to avoid KYC programs. Possibly the most discreet way of accomplishing this is through Bitcoin ATMs. These machines exchange cash for bitcoin and charge a substantial fee (on average 8.4 percent).⁵ A client deposits cash into these machines and receives a wallet number with the amount of bitcoins equal to their deposit minus a fee. There are also websites⁶ that will convert payment from one source (e.g., credit card) to credits, for the purposes of buying online adult classified ads. These websites essentially work as brokers that convert fiat currency into bitcoins. Finally, even gift cards can be used to purchase these credits through the use of websites that provide these online conversion services.⁷

³ Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another.

⁴ Referenced from coinmarketcap.com on April 10, 2016, <https://coinmarketcap.com/>

⁵ <https://coinatmradar.com/blog/tag/fees-2/>

⁶ <https://buybpcredits.com/do-i-need-bitcoins/>

⁷ <https://paxful.com/backpage>

Successful law enforcement investigations involving cryptocurrencies are often aided by services from private companies that track and rate cryptocurrency activity. Many companies offer these services and there are public-private partnerships that help players in the blockchain industry connect with law enforcement worldwide.

Public-private partnerships

Alan Cohn, from the Blockchain Alliance (a forum for industry, law enforcement and regulatory agencies for the combatting of criminal activity on the blockchain), gave an overview of the goals and services that this group provides. Cohn explained that the inspiration for the Blockchain Alliance stemmed from the lessons learned in the early days of the internet, when criminals exploited the technology for heinous crimes like child pornography. Given the novelty of the internet in its early days, law enforcement reached out to the industry for training and guidance. This time around, the industry has reached out to law enforcement proactively to promote responsible uses of the new technology.

The Blockchain Alliance brings together some of the most lauded players in the blockchain ecosystem to serve as a resource for law enforcement and regulatory agencies. It offers education, technical assistance and informational sessions about the uses of blockchain technology. It has garnered support from industry players including miners, exchanges, analysis companies and many others who participate in this open forum to help combat criminal activity. The alliance also counts law enforcement and government agencies, such as the U.S. Department of Justice, the U.S. Department of Homeland Security Investigations, the U.S. Federal Bureau of Investigation, the U.S. Secret Service and many other parallel international organizations as partners.⁸ The group serves as an excellent example of

the synthesis needed to help to ensure safe growth and adoption of blockchain technologies through awareness of regulatory necessities and a constructive relationship management with law enforcement.

Government interest

A blockchain's accurate accounting and tracking abilities can be used for a plethora of different tasks. Government interest for blockchains shows just how many different uses this technology can have. At the Chicago event, Jennifer O'Rourke, from the Innovation & Technology at the Illinois Department of Commerce, and Ciccolo discussed the "Illinois approach" to blockchain. This approach is one that leverages private and public relationships to examine how to advance possible blockchain-related applications without curtailing growth with premature legislation. In fact, the Illinois Department of commerce has begun researching to see if blockchain could be used in the future to house government records.

As governments further explore blockchain solutions, financial institutions may also begin to review potential clients differently. At the Chicago event, Michael Busch of Burling Bank discussed his institution's yearlong research of the Bitcoin industry, which continues to this day. Such research includes studying the different types of businesses that use blockchains and or cryptocurrencies in their operations. As time passes and greater knowledge is acquired, banking blockchain companies may become less dichotomous if careful reviews of business models are completed in order to recognize companies that offer less money laundering risk.

In the Toronto event, central banker James Chapman from the Bank of Canada displayed the platform the central bank created to simulate central bank loans to banks. The central bank used the Ethereum blockchain, the

world's second largest blockchain by market cap, to create a system where the central bank can create virtual currency, loan it to banks and destroy it. There is no immediate plan to adopt such a platform, but the government's interest in the technology should serve to remind the reader that the technology is likely here to stay.

The way forward

The blockchain industry has quickly matured since the creation of the first blockchain in 2009. Entrepreneurs have largely replaced the rebels who once touted the need for a completely deregulated currency that functioned outside the purview of government, law enforcement and regulators. Compliance is now recognized as a fact of life by most successful companies and AML regulations are an important part of this recognition. The presenters and organizers of the Chicago and Toronto events propagate the need for open dialogue on blockchain and cryptocurrency in order to bridge the gap between the industry, law enforcement and regulators. Educating AML professionals and law enforcement of the various risks and solutions that exist in this space helps to ensure that innovation does not come at the expense of public safety. Communicating trends and indicators of crimes and risks associated with blockchain technology and cryptocurrency transfers helps to enhance reporting standards and criminal investigations and increase public safety. It is important that AML professionals continue learning about this technology. 

Leonardo Real, CAMS, manager—AML, Bank of Montreal, Toronto, Ontario, Canada, leonardo.s.real@gmail.com

Advisor: Joseph Mari, CAMS, senior manager for major investigations, Bank of Montreal, Toronto, Ontario, Canada, joseph.mari@bmo.com

⁸ Luke Parker, "Controversy Arises as New Blockchain Alliance Engages with U.S. Law Enforcement," Brave NewCoin, October 24, 2015, <https://bravenewcoin.com/news/controversy-arises-as-new-blockchain-alliance-engages-with-us-law-enforcement/>

ACAMS® | CHAPTERS



The ACAMS Chapter Development Program aims to focus the association's international efforts in anti-money laundering education and training at a local level. Chapters foster professional relationships and provide local forums for discussion around region-specific issues.

**Chapters launching soon*

Cultivating Comradery Worldwide



Find a local ACAMS chapter near you or start one today!

www.acams.org/chapters | chapters@acams.org



ARTIFICIAL INTELLIGENCE:

The implications of false positives and negatives

Does overthinking artificial intelligence result in self-inflicted suspicious activity reports (SARs)? Financial institutions not only pride themselves but are obliged to document when consumer activity goes astray. SAR authors who have an overreliance on the results of anti-money laundering (AML) detection/risk assessment software dutifully draft the then required-per-policy SARs. These reports then spur a chain reaction of events that impact not only the customer, but the financial institution and law enforcement alike. But what are the ramifications when financial institutions become victims of their own policies that are based on default artificial intelligence rather than due diligence? What are the possible implications of a misinterpretation of otherwise legitimate customer transactional activity?

False positives

Frequently, automated transaction monitoring systems will alert AML investigators when a customer conducts cash withdrawals in a pattern indicative of possible structuring. This pattern often consists of the customer(s) conducting cash withdrawals on the same, consecutive or closely consecutive days at either the same or multiple branches. At face value, this pattern would appear to be suspicious and potentially unlawful. A SAR would be filed on this customer, as there is an appearance of high-risk behavior. But what does this first SAR mean? Clearly, this customer will become subject to frequent review. Each review will scrutinize the customer's transactional activity. Should this seemingly suspicious transactional behavior occur again, the customer relationship could

be subject to termination. Multiple SARs could attract the interest of law enforcement. This ripple effect would likely trigger law enforcement to generate a subpoena for records and documents. From there, time will pass and when the records are produced, a bill will be attached with an expectation of swift payment. Investigators will then invest time—to the detriment of other cases on their desk—to craft a spreadsheet reflective of the suspicious transactional data as well as produce a line of questioning for witnesses and suspects alike. A secondary officer will then be requested to backup and respond (now without delay) to the first branch location with the lead investigator. Officers will interview a teller as to any knowledge about the customer or if they recall any details with regard to the suspicious transactional activity that was the basis for the

SAR in the first place. An anxious teller will agree to answer the questions and then, and only then, the investigators will learn that the circumstances behind this “activity” was actually created by the bank and not the customer.

The financial institutions had a posted “cash back” limit below the CTR level. The customer needed more cash than could, or would be, provided by the branch. The lack of funds at the first branch was the stimulus for subsequent visits to other branch locations and cash withdrawals. This revelation affirms there was no intent to commit the suspected structuring captured by the monitoring software. It was just an attempt to obtain the necessary funds as expeditiously as possible. The customer was not engaging in criminal conduct, but without initial examination executed by the AML investigators, the

customer became falsely labelled as a risk and subject to undue scrutiny by not only the financial institution but now law enforcement. An initial query by the AML section would have de-risked this customer saving both time and money—two commodities that are precious to law enforcement and financial institutions.

While bulk cash withdrawals in and of themselves may seem unusual, there are still legitimate businesses and professions that are frequently subject to this scrutiny, but never afforded exculpatory considerations. Worse, know your customer (KYC) documentation may not capture this information as it is often associated with a secondary occupation.

For example, private ATM operators are often subject to short notice on if, and when, bulk currency will be needed for their machine(s). Withdrawals have been observed from both business and personal accounts on same, consecutive, and/or closely consecutive days at the same or multiple branch locations in order to satisfy the funds necessary for their side business. Although there are AML considerations with private owner-operated ATM businesses, the majority still remain a legitimate business venture.

Private ticket services and agencies often work on short notice as to when the tickets for the “hottest shows” or popular sporting events become available. These business owners are in need of immediate currency and have been found to take extensive, but ultimately legal, measures to achieve the necessary funds for the ticket purchases that may make or break this now proper version of “ticket scalping” business ventures.

Updated or even supplementary KYC customer contact, in addition to communication with the particular branch(es) regarding the date(s) of the suspicious transactional activity would have correctly categorized the above described customers. These preemptive measures would likely increase the probability of preserving a banking relationship with the account holder(s) and eliminating a false positive(s).

Dependence on the algorithms of artificial intelligence without verification can come at a cost

False negatives

As frustrating as it may be to have exhausted law enforcement and financial resources on an investigation that could have been resolved at the onset of detection, worse is the unexposed “false negative.” The seemingly low-risk profile, which poses little to no exposure for the financial institution, possesses high-risk indicators of criminal activity.


Many compliance and risk assessment monitoring systems are equipped to mitigate risk on behalf of the financial institution, but some fail to identify the accounts and/or customers engaging in unusual, but not necessarily suspicious, activity that would trigger a SAR filing.

The first example is a business account for a used car dealership. This typical account profile is not immune to cash deposits. In fact, U.S. currency for used vehicles is a common business practice. However, when a West Coast used car dealership is receiving multiple cash deposits into their business account from outside the geographic location it would take the scrutiny of an experienced AML investigator to recognize it is unlikely that customers were buying used vehicles, only to then pay shipping fees (or drive cross country) for said vehicles. It would be logical to infer the same, or at least similar, vehicle would be for sale within the geographic footprint of the out-of-state customers. Monitoring programs can and have overlooked this very profile, as there was no loss to the financial institution. However, there were numerous financial losses to the victims of various false pretenses. It was not until one victim finally

recognized he/she was duped and had the courage to report this (in hindsight) scam, did law enforcement initiate contact with the financial institution to report the criminal activity. Only then did law enforcement from various states and the financial institution work in conjunction to dismantle the criminal organization and attempt to make the victims whole.

The second example is a personal account assigned to an East Coast customer. The account was receiving nominal amount wire transfers reflecting the subject matter as “family support.” In addition, out-of-state cash deposits were also transacted into this account. At face value, this would appear to be overly generous efforts to support a loved one. Again, there was no loss to the financial institution and no SAR filed on the customer or the account. Had a SAR been filed, AML investigators and law enforcement alike would have quickly discovered the account from where the “family support” wires originated was partially funded by yet another victim who was hoodwinked in a real estate scam. Had either of these accounts been identified as suspicious at the emergence of the wires and out-of-state cash deposits, there would have been a chance that all the funds could have been traced and seized pursuant to court orders. Instead, law enforcement, with the assistance of AML investigators, were only able to trace and retrieve a percentage of funds.

Conclusion

False positives and negatives can and have gone unnoticed by detection programs. Dependence on the algorithms of artificial intelligence without verification can come at a cost. From failure to de-risk a customer to discounting suspicious accounts that pose no loss to the financial institution, there is room for negligence but also opportunity for reformation. To error is technology but to mitigate risk is divine. 

Stacey Ivie, M.Ed., task force officer, Washington Baltimore HIDTA, Northern Virginia Financial Initiative (NVFI), Annandale, VA, USA, sivie@wb.hidta.org

ISLAMIC TERRORISM FROM A RISK PERSPECTIVE

Governments, through their intelligence and law enforcement agencies, assess and prepare for terrorist activity based on the level of the risk or physical threat that terrorism presents. To address the risk or the threat, you have to understand the risk or the threat. Understanding the threat of terrorism can lead to detection, intervention, disruption and prevention. Truly understanding requires accurate and continuous risk assessment. No one is more cognizant of the risk assessment process than financial institutions. The cornerstone of every anti-money laundering (AML) compliance program is the risk assessment.

An AML risk assessment is designed to identify inherent risks. Once inherent risks are identified, you develop controls or control environments that will mitigate risk. The next step in the process is to identify the inevitable residual risk. Once residual risks are identified, you again determine the level of controls necessary to continue to mitigate the risk. In assessing the threat of terrorism from an AML perspective, you must first assess the overall threat of terrorism and then drill down and assess the terrorist financing risk. Terrorist financing should be considered a component of terrorism, and therefore, should be assessed in conjunction with the broader terrorism risk and mitigation strategies.

Specific inherent and residual terrorist risk factors are not financial institution risk factors. As a component of terrorism, terrorist financing risk factors should be considered after assessing the specific terrorist risk factors by drilling below the broader terrorist risk factors to identify the

financial threats. However, it should be noted that inherent and residual mitigation measures will include specific financial disruption mechanisms.

The greatest immediate threat to the U.S. and our allies comes from jihadist terrorism or Islamist extremism. Islamism is a radical political ideology. It is extremely important to note that Islamism is separate from Islam as a religion. Islam is not the problem. Jihadist extremists who twist Islam and misinterpret it to fit their radical ideology present the problem. Core groups, most notably the Islamic State and al-Qaeda, their affiliate groups and grassroots jihadists who are influenced by these groups pose the threat. Groups like the Islamic State and al-Qaeda have been extremely adept at exploiting the internet for propaganda, fundraising, and most notably, recruitment. Disenfranchised and easily radicalized individuals, who become foreign terrorist fighters and homegrown violent extremists, have evolved into the most acute threat to the U.S. and its allies.

On April 18, 2017, in a speech at George Washington University, Center for Cyber and Homeland Security, Department of Homeland Security Secretary, John Kelly, discussed the threat of terrorism. Secretary Kelly made the following comments: "The threat to our nation and our American way of life has not been diminished. In fact, the threat has metastasized and decentralized, and the risk is as threatening today as it was that September morning almost 16 years ago. As I speak these words the FBI has open investigations in all 50 states...But the dangers don't just come from overseas. Over the past few years, we've seen an unprecedented spike in homegrown terrorism. In the past 12 months alone, there have been 36 homegrown terrorist cases in 18 states. These are the cases we know about—homegrown terrorism is notoriously difficult to predict and control. And what's feeding this homegrown violence? Most experts agree a major contributor is the internet."¹

Secretary Kelly's remarks underscore the fact that over the past several years, the terrorist threat environment facing the U.S. and its allies has evolved into something more dangerous and complicated than ever before. It points to the threat evolution of homegrown violent extremists. In order to disrupt, diminish and ultimately prevent the threat of homegrown violent extremism, we must fight the threat of terrorism through sustainable tactical and strategic strategies. Sustainable tactical and strategic strategies require establishment of meaningful public-public and public-private partnerships.

¹ "Home and Away: DHS and the Threats to America, Remarks Delivered by Secretary Kelly at George Washington University Center for Cyber and Homeland Security," U.S. Department of Homeland Security, April 18, 2017, <https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america>



We must establish and maintain tactical measures to thwart terrorist attacks. Tactical measures include:

- Public sector intergovernmental offensive and defensive activities to include military action, diplomatic engagement, intelligence operations, law enforcement investigations and sanctioning actions
- Public and private sector capacity building initiatives to assist at-risk countries build good governance systems and to fight corruption
- Public and private sector financial disruption activity through disrupting the funding flows to and from terrorist organizations. This is where financial institutions, and more broadly the financial services industry, play a significant role

We must establish and maintain strategic measures to counter the extremist radicalization that fuels its hatred and violence and undergirds its strategy and global appeal. Strategic measures include:

- Public and private sector community outreach and vigilance to identify and interdict individuals at risk for radicalization

- Public and private sector propaganda strategies using social media and internet communications to dispel and counter the appeal of radicalization
- Public and private sector strategies to prevent radicalization, promote intervention and reintegration

The foundation for developing meaningful and sustainable tactical and strategic strategies is to understand the risk factors. You understand risk factors through risk assessment and analysis. From an AML perspective, you identify the inherent risk factors, risk mitigation of the inherent risk factors, residual risk factors and risk mitigation of the residual risk factors. For Islamic terrorism the inherent risk factors include: sectarianism, ideology, lack of governance, corruption and convergence. The residual risk factors include adaptability, capacity and reach.

Inherent and residual risk factors for Islamic terrorism do not contain direct financial threats. The financial threats are indirect. This is one of the reasons why terrorist financing is a component of terrorism. From an AML perspective, this is also one of the primary considerations as to why terrorist financing is so difficult to identify. Developing tactical

and strategic Islamic counterterrorism strategies begins with assessing and understanding terrorist risk factors starting with inherent risk factors. Tactical strategies will be more tangible, while strategic strategies will be more intangible.

There are a variety of inherent risk factors that merit consideration. Five fundamental inherent risk factors include:

1. **Sectarianism:** Sectarianism goes back thousands of years. It goes back to the death of the Prophet Muhammad in the year 632. It is rooted in the divide between Sunni Muslims and Shiite Muslims about who was the rightful successor to Muhammad. Through the years, the sectarian divide between Sunnis and Shiites has grown and has led to significant fighting, chaos and instability in the Arab world.
2. **Ideology:** Islamist ideology is an extreme radical interpretation of Islam that has been adopted by Islamic terrorist groups to justify their violent tactics and political quest to establish a caliphate.
3. **Lack of governance:** The lack of governance in many countries is caused by factors to include the

Sunni and Shia divide and corruption. The lack of governance creates crisis and chaos, which serve as an incubator for the growth of terrorist groups and transnational criminal organizations.

4. **Corruption:** Corruption contributes to a lack of governance and a loss of trust. When the public does not trust the government there is a lack of governance, which fosters sectarianism and enables the growth of terrorism and transnational criminal activity.
5. **Convergence:** The convergence of terrorist groups and transnational criminal organizations has proven to be extremely profitable for both. By forming hybrid terrorist and criminal organizations, these groups have been empowered and have developed lucrative funding streams, especially in countries with poor governance.

Each of the five inherent risk factors build on each other to enhance the risk of Islamic terrorism. The tactical mitigation strategies to address the inherent risk factors should first be focused to operationally contain the physical threat of terrorism. It should then lead to disruption, and ultimately, to prevention, in tandem with strategic strategies.

There should be two prongs to the tactical mitigation strategy. The first requires public sector interagency collaboration to continue to contain and disrupt the threat of terrorism through military, diplomatic, intelligence, law enforcement and sanctions operational counterterrorism measures. The second prong requires public and private sector collaboration to disrupt and prevent the flow of funds to and from terrorist organizations, operations and operatives. This is where financial institutions play a pivotal role.

Strategic mitigation strategies should also be two pronged. Both prongs require public and private sector partnerships. The first prong should involve public and private sector collaboration to counter the propaganda used by terrorists on social media and through internet communications for recruitment. The second prong should involve diverse community outreach to identify at-risk individuals and to interdict those who fall prey to jihadist recruitment. This requires vigilance, intervention and ultimately the reintegration of at-risk individuals back into the community.

There are two primary Islamic terrorist residual risk factors, which are:

1. **Adaptability:** All terrorists, including Islamic terrorists, have demonstrated the ability to be adaptive. As the public and private sector assess risk, terrorists assess counterterrorism tactics and adapt their operations to avoid detection and disruption. They also seek to continuously identify systemic vulnerabilities they can exploit in order to sustain the threat they pose.
2. **Capacity and reach:** Islamic terrorist groups evolve or devolve as their capacity and reach change. For example, the Islamic State evolved into an organization with a supposed caliphate, which provided barbaric governance. As the caliphate collapses, the Islamic State will devolve from a structured organization to an insurgency. Their capacity to govern will cease but their ability to wreak havoc will continue to some extent. Through homegrown violent extremists and other mechanisms, they will strive to establish greater reach by causing attacks in the U.S. and allied nations.

To address the residual risk, both the tactical and strategic mitigation strategies should continue to follow their two-pronged approaches. Terrorists will be more adaptive to tactical counterterrorism initiatives. Therefore, from a tactical counterterrorism perspective the response should be more vigilant and flexible to adjust to the adaptations of the terrorists. As Islamic terrorist groups, most notably the Islamic State, see their physical presence in Iraq and Syria diminish, they are more likely to push outward on the internet to intensify recruitment of homegrown violent extremists. Between foreign fighters returning to their homelands—from Iraq

and Syria—and the ongoing recruitment of homegrown violent extremists, the Islamic State will encourage them to commit terrorist acts in their home countries. Thus, it is critically important that strategic counterterrorism initiatives intensify to identify, interdict and disrupt the radicalization process.

The ultimate goal of counterterrorism initiatives is to eliminate the threat of terrorism. Unfortunately, that will never happen. With respect to Islamic terrorism, especially with the serious sectarian divide between Sunnis and Shiites, it is extremely unlikely that we can eliminate the inherent and residual risk factors. However, we can work toward detection, intervention, disruption and prevention. To accomplish this, we must understand the enemy, their perspective and the risks they pose. As part of this process, we must identify and understand the flow of funds to and from terrorist organizations. This should emphasize the importance of financial intelligence and the risk assessment process.

Understanding the terrorist threat should lead to the development and implementation of effective tactical and strategic containment and disruption strategies. These initial strategies are mostly reactive strategies that can be built upon. This is the juncture where public-public and public-private partnerships play a meaningful role. This is where collaboration leads to the development of more proactive strategies that leverage the capabilities and capacity of public and private partners. This will allow us to evolve from reactive containment and disruptive strategies to reactive and proactive disruptive and preventive strategies. We may never be able to eliminate the threat of terrorism, but we can disrupt and prevent terrorist attacks from occurring. It is a daunting task that begins with understanding risk. **A**

Dennis M. Lormel, CAMS, internationally recognized CTF expert, president & CEO, DML Associates LLC, Lansdowne, VA, USA, dlormel@dmlassocllc.com

ACAMS® | Certificates

Convenient, online, mixed-format training for compliance teams of all sizes ranging from early to intermediate career levels.



Transaction Monitoring



Trade-Based Money Laundering



Cyber-Enabled Crime



Sanctions Compliance



KYC CDD



Counter-Terrorist Financing (CTF)



AML Foundations

Participants who successfully complete ACAMS Certificate courses receive:

- A certificate of completion proving their commitment to protecting their institutions against money laundering, terrorist financing and other financial crimes.
- Four CAMS credit hours to keep them on track towards CAMS certification or CAMS recertification.

Earn your training certificate: acams.org/certificates

THE ROAD TO MONEY LAUNDERING CENTRICITY

Among federal crime fighters, money laundering has become a big deal. Both the Federal Bureau of Investigation and the Drug Enforcement Administration have made combating money laundering one of their top priorities. Factor in the work of the Internal Revenue Service Criminal Investigation (IRS-CI) and the Department of Homeland Security and it is clear that the federal government is deploying a battalion of financial soldiers to hit criminals where they are most exposed: their money trails.

Within arsenal U.S. criminal statutes, the crime of federal money stands out as a rather potent weapon. These laws imposed long prison terms and the authority to seize assets derived from illicit proceeds—something criminals particularly disdain. Using the money laundering offense also brings down the enablers—the professional money launderers who work in the shadows to keep the criminals off law enforcement’s radar. Without those skilled in moving, concealing and cleaning ill-gotten gains, the potential for criminal organization growth is stunted.

Adding the predicate offense of money laundering in a major drug case is gamesmanship. There is no better way to link a crime boss to underlings and paint the enormity of the criminal enterprise than leading a jury down the path of a criminal’s money trail. This is where jurors usually have their “ah hah moment.” The money laundering evidence is like nails to a chalkboard to defense attorneys.

It is not just drug money

Based on the U.S. Treasury Department's 2015 national money laundering risk assessment, the total illicit funds generated in the U.S. annually is estimated at \$300 billion. That is a lot of bad money that needs to be washed, so that criminals can enjoy the fruits of their felonious acts without such expenditures biting them in the rear extremity.

What may be a surprise to the lay person is that for every dollar earned by a drug dealer, three dollars are earned by fraudsters. Fraud has become the reigning king of illicit income attracting a host of unsavory criminal groups. And just like drug cartels, domestic and transnational fraud enterprises have an insatiable need for money laundering services. This is why the FBI's Money Laundering Unit focuses on third-party facilitators, such as attorneys, accountants and brokers. The FBI reminds the public that money laundering not only fuels organized crime, but it also facilitates significant tax evasion.

The dominant platoon in the fight against money laundering, in particular with fraud, continues to be IRS-CI who has honed the art of sculpturing complex money laundering cases on a variety of criminals. IRS-CI agents cut their teeth on tax evasion cases where dollars on and off the books are traced beyond a reasonable doubt and where transactions are not left to chance.

As law enforcement has become more proselytized to the virtues of money laundering investigations to address a wide array of criminal activity, their reliance has grown on suspicious activity reports (SARs) filed by financial institutions, a regulatory requirement under the Bank Secrecy Act. That has emboldened regulators to levy fines in the billions to financial institutions that have been willfully derelict in their duty to maintain an adequate anti-money laundering program that detects, reports and prevents money laundering. Western Union is the latest to pay a hefty penalty of \$586 million for willful blindness of "clear evidence" of widespread money laundering associated with elder abuse fraud.

The early days

The story starts back in the late 1920s when law enforcement was stymied in their efforts to bring down the leaders of large-scale organized crime. The conviction of Al Capone, the world famous kingpin gangster, opened the government's eyes to using tax evasion to defeat criminally elite gangsters. President Herbert Hoover was so impressed with the outcome that he ordered the Intelligence Unit (now IRS-CI) to go after all the other public enemy number ones throughout the country. President Franklin D. Roosevelt gave similar marching orders and was so pleased with the results he sent the head of the Intelligence Unit, Elmer Irey, a personal thank you letter praising their "incorruptibility" and "A-1" efficiency.

Learning from the existential mistakes of other kingpins, the smarter crime bosses began hiring attorneys and certified public accountants to devise schemes to hide profits and assets from the pesky IRS agents who were opening audits on gangsters in droves. These money laundering

professionals already honed their skills by hiding profits for certain wealthy taxpayers who did not want to pay their fair share of income taxes.

A well-oiled machine

By the 1960s, professional money launderers had perfected a series of money laundering best practices to keep their criminal enterprises humming along. And through this copious money laundering criminal organizations got bigger and worse. Couriers were used to deposit currency from illegal drugs, prostitution, racketeering, sports wagering and loan sharking in shell company bank accounts. The illicit proceeds were then transferred to other dummy companies until they were sufficiently layered in complexity. The ill-gotten profits eventually made their way to Swiss bank accounts.

Once the illicit proceeds were pocketed away in Switzerland, the money trails were out of reach of U.S. law enforcement. The funds were eventually repatriated back by disguising transactions as loans or other innocuous payments. Some enterprising gangsters just bypassed the domestic banks and had their couriers fly directly to Switzerland or just took a quick jaunt to the Bahamas where Swiss-affiliated banks welcomed them warmly.

The first major assault

In response to increasing reports of people bringing bags of currency of "doubtful origin" into banks and citizens using the bank secrecy laws of other countries to conceal illegal activities, in 1970, former President Richard Nixon signed into law the BSA. Banks now had to file a currency transaction report (CTR) to report transactions of \$10,000 or more in a single day. BSA also required anyone traveling in or out of the country to declare currency (domestic or foreign) of \$10,000 or more. And to pull the noose a little tighter, BSA required taxpayers to declare the ownership in foreign bank accounts. The primary purpose for BSA was to give the IRS the upper hand in tracking the money trail.

With the onset of BSA, banks had the uncomfortable task of asking their valued customers for identification and inquiring whether the transaction was on behalf of another. This was often met with the following response among a certain ilk of secretive depositors, "None of your business." Not wanting to turn away valued customers, several banks purposely fell asleep at the compliance wheel. At this

The problem with tax evasion cases is that they did not yield long prison sentences and they took a significant amount of time to put together

time, BSA did not impose biting civil or criminal penalties and to some in the banking industry, willful blindness fit their model of acceptable risky behavior.

As the government became more focused on the expanding drug trade, former President Gerald Ford, ordered that a tax enforcement program be initiated for high-level drug trafficking. In his message to Congress, Ford pointed out the obvious reason why legislators should support the endeavor of unleashing more tax cops, "We know that many of the biggest drug leaders do not pay income taxes on enormous profits."

Ford's tax evasion battle plan bore out of frustration with coy drug dealers who oversaw the distribution of narcotics. The beauty of tax evasion cases is that they did not focus on the movement of contraband but rather unexplained wealth—a much harder evidentiary trail to cover up. The problem with tax evasion cases is that they did not yield long prison sentences and they took a significant amount of time to put together. But to the liking of drug task forces, IRS auditors were able to make a 50 percent jeopardy income tax seizure of a crook's cash if the suspect claimed he had no idea how the cash got there and who owned it.

Drug dealers and those annoying CTRs

American marijuana and heroin dealers realized their the best course of action to deal with BSA was to befriend witting banks who were more focused on profits than compliance, a fact not lost to IRS-CI. Great American Bank of Dade County Florida was caught failing to file CTRs on \$96 million in currency transactions relating to drug proceeds. First National Bank of Boston failed to report \$1.2 billion in currency transactions much of which was \$20 bills stuffed in bags and placed on planes destined for Switzerland. And then there was former city councilman George Thompson III—the chairman of the board of the Ridglea State Bank who was sent to prison for three years for knowingly assisting a drug dealer to avoid CTRs. It did not help Thompson's defense that this drug dealer was supplying narcotics to Thompson's mistress.

By the 1980s, America saw the rise of even bigger and worse criminal enterprises ruled by ruthless international kingpins such as Carlos Escobar whose henchmen caused the murder rates in Miami to skyrocket. The Columbia Cartels and their chain of American distributors were generating not bags but palettes of cash. Escobar found a very friendly bank, Bank of Credit and Commerce International (BCCI), that was more than willing to help the drug dealer who *Forbes* labeled one of the richest men in the world.

Taking advantage of the heat the Feds where putting on banks, the enterprise General Manuel Noriega offered a safer alternative to the U.S. banking system where there was no such thing as a CTR. Panama—where U.S. dollars are recognized as legal tender—soon became a money laundering hub where private jets from Florida landed like clockwork packed with currency.

In 1984, U.S. Customs agents searched a suspected Learjet headed to Panama and found \$5.4 million in undeclared cash. They also found the chief money launderer for the Cali Cartel, Ramon Milian Rodriguez, responsible for laundering up to \$350 million from 1979 to 1983. After his conviction, Rodriguez told U.S. officials that the cartels paid Noriega \$10 million a month in exchange for unfettered access to their banks plus the identity of DEA agents working in Panama.

The criminalization of money laundering

To address the growing money laundering problem, former President Ronald Reagan signed into law the Money Laundering Control Act in 1986. The law made money laundering a federal crime with significant prison time and provisions to seize assets if derived through illicit proceeds. Now, if a drug dealer tried to avoid a CTR or tried to hide,

clean or transfer dirty money, it could land him a very long stay in a spartan room at a federal correctional facility.

Several large-scale operations were instituted targeting the money laundering tentacles of the cartels in an effort to hit the organizations where it really hurt. U.S. Customs led a multi-year operation called "C-Chase" where their star undercover agent infiltrated Escobar's money laundering machine and became one of their chief money launderers. The dramatic take down of Operation C-Chase reads like a Hollywood screenplay where an elaborate wedding was staged as a ruse to lure all the criminals in one place. Operation C-Chase brought down senior executives of BCCI, and ultimately led to the downfall of the once mighty bank. The story was too enticing for Hollywood to pass up so they made it into a movie called, *The Infiltrator*, starring Bryan Cranston from the hit TV show, *Breaking Bad*.

Operation Dinero was the brainchild of the DEA and IRS who had the ingenious idea to set up their own dirty bank to attract money launderers seeking morally deprived financial institutions. Their odious smelling bank attracted more money laundering flies than an unkempt horse stable. The operation yielded 88 coordinated arrests worldwide, \$52 million in seizures and more importantly, a treasure trove of intelligence on the interworking's of the cartel money laundering apparatuses. Rumor has it there is a movie in the works on this case too.

Trying to stay off the radar

When it came to their toys, drug dealers were just bypassing banks and buying cars, boats and jewelry with cash. In Miami, it was hard to find a deal on a luxury car because drug dealers had no problem paying sticker price. In response, Congress mandated car, boat and jewelry dealers to report cash sales over \$10,000 to the IRS on Form 8300. President Reagan's Money Laundering Control Act also made it a crime to file a false CTR or 8300.

The owners of AMS Auto Sales—tucked away in a neighborhood where most were on welfare struggling to make ends meet—had a robust business selling Ferraris, Mercedes and Rolls-Royces

until the Highway Patrol tipped off the IRS. The ensuing undercover investigation revealed that AMS almost exclusively sold to drug dealers who purchased the high-end vehicles with cash or drugs and then resold the cars to clean their proceeds. The owners went down for failure to file Form 8300 and the IRS seized the entire dealership. There were other dealerships like AMS festooned across the country and many were taken down through undercover operations where agents posed as obvious drug dealers. As one IRS senior manager quitted, “It was like shooting fish in a barrel.”

The ever-resourceful criminals figured out that by spreading currency transactions among numerous individuals with smaller deposit amounts (a technique known as smurfing) made it harder for law enforcement to piece together the organization's money trails. IRS and Customs agents engaged in robust outreaches to banks encouraging them to report structuring activity, such as smurfing. To their credit, many banks volunteered significant leads but there were some not imbued with the sense of doing the right thing. In 1996, Congress mandated that banks file SARs to report suspicious activity indicative of structuring, money laundering and tax evasion. The SARs proved to be highly useful in identifying money laundering schemes.

As the new millennium approach

The Columbia Cartels eventually decided the best course of action was to just wholesale the cocaine and use the Mexican cartels to handle the distribution of the white powder into the U.S. and related retail operations. All of a

sudden there was a money laundering demand to get drug currency south of the border and converted into pesos. In response, the government required all money services businesses, such as wire remitters and check cashiers, to fall under the provisions of the BSA. Check-cashing businesses need a lot of currency so cartels found businesses willing, for a fee, to trade the endorsed checks they got from customers for dirty cash. The criminals would then benignly deposit the checks into bank accounts avoiding CTRs.

In 2001, when former President George Bush signed into law the USA PATRIOT Act, it extended the role of banks to detect, report and prevent money laundering. In response, banks established financial investigative units to conduct due diligence inquiries and real time transaction monitoring. In the subsequent decade, casinos, mutual funds, securities brokers, insurance companies and operators of credit card systems were all mandated to comply with the anti-money laundering provisions of the USA PATRIOT Act. As a result, financial institutions became sort of mini investigative arms of the federal government.

Money laundering—Greatest hits


Since the enactment of the money laundering laws, the Hall of Fame of indictments include: Noriega the despotic Panamanian dictator; the Orejuela brothers, the more successful successors of Escobar; the head of the Tijuana Cartel; and one of the most infamous gangster warlords of our time, El Chapo.

Over the past three decades, the money laundering laws have played a critical role bringing down massive Ponzi schemes, embezzlements, mortgage fraud, political corruption and human trafficking. One of the many honorable mentions goes to General Electric who in 1992 pleaded to money laundering in connection with a massive defense contractor fraud. One could argue that money laundering statutes have been more effective in debilitating criminal groups than the provisions of the Racketeer Influenced and Corrupt Organizations Act, which was enacted the same year Richard Nixon enacted the BSA.

The takedown of Liberty Reserve, a virtual currency exchange house that laundered \$6 billion of illicit proceeds reveals the extent of where money launderers are beginning to coalesce in the digital age. Former Chief of IRS-CI, Richard Weber, told reporters that “If Al Capone was alive today, this is how he would launder his money.”

Conclusion

The money laundering laws penned into action by Ronald Reagan were mirrored around the world by governments attempting to combat entrenched criminal activity and corruption. Imitation is the highest form of flattery. In breaking down the walls of financial subterfuge, money laundering violations became the Sherman tank in the fight against entrenched criminal organizations. However, this criminality destructive vehicle relies on a sturdy undercarriage—an undercarriage made up of numerous financial institutions deploying AML programs to detect, report and prevent money laundering.

As any seasoned federal money laundering investigator will tell you, the vast majority of money laundering cases resulted from information gleaned from CTRs and SARs. As the government lauds the value of money laundering prosecutions we should never lose sight that a good portion of the success is attributable to the dedicated work of numerous AML professionals ensuring the quality of BSA information. As with many battles of consequence, in the war against money laundering there are a lot of unsung heroes. 

In 1996, Congress mandated that banks file SARs to report suspicious activity indicative of structuring, money laundering and tax evasion

Paul Camacho, CAMS, vice president of AML compliance, Station Casinos LLC, Las Vegas, NV, USA, paul.camacho@stationcasinos.com

Joann Alicea:

The fight against human trafficking/ smuggling continues

A *CAMS Today* caught up with Joann Alicea, CFCI, senior compliance officer at JPMorgan Chase, to discuss the horrific offenses of human trafficking (HT) and human smuggling (HS), and how the public and private sectors can work together to effect positive change and help shape the future of suspicious activity reporting.

Alicea has over 10 years of regulatory compliance fraud/anti-money laundering and risk experience in monitoring bank accounts, prepaid cards, and merchant and cardholder credit card transactions. She has received commendations for excellent investigative work from the U.S. Secret Service and Homeland Security Investigations (HSI) for assisting in domestic and international fraud/money laundering cases.

In addition, Alicea has written two *ACAMS Today* articles on HT and she is a public speaker on fighting the crime of HT at both the Visa and MasterCard payment level and on victim money laundering scams. For the past six years, Alicea has held a very public lobbying campaign to encourage the Financial Crimes Enforcement Network (FinCEN) to consider an update to the SAR form to include a checkbox for HT/HS.

ACAMS Today: Could you give our readers a brief glimpse into your background?

Joann Alicea: I became a financial crimes investigator shortly after the 9/11 attacks. Prior to this, I was a credit card fraud analyst. The 9/11 attacks highlighted the importance of information sharing between financial institutions and law enforcement. Very quickly my role within the financial institution transformed from being fraud specific to being more holistically focused on the identification and reporting of financial crimes and terrorist financing. The Office of Foreign Assets Control screening and SAR filing responsibilities were now part of my daily job responsibilities—before 9/11 neither had been my responsibility.

AT: When did your passion for the prevention of HT begin?

JA: My interest started while performing a routine investigation in 2010. I became aware of the use of prepaid cards on sites like Craigslist and Backpage.com for all sorts of criminal offenses, including, but not limited to, prostitution and HT. The fact that financial transactions for prostitution and HT were being transacted through banking products fascinated me. I began to watch news documentaries on HT such as *CNN's Selling the Girl Next Door*. I sought out and watched HT education movies. In addition, I attended anti-HT conferences around the country. It was at these conferences where I met actual survivors of HT, which fueled my passion on the subject. I began to read extensively on the topic. *ACAMS Today* was a fantastic source of information in 2010 and continues to be a powerful source of up-to-date, reliable information on all sorts of trafficking, including forced labor, sex trafficking and indentured servitude.



AT: You worked extensively to gather a lot of knowledge on this horrific crime. What was your next step and how did you plan to put your knowledge to use?

JA: Well, my first step was getting recognized in the industry. I received an invitation from a law enforcement HT detective to join a LinkedIn Human Trafficking Investigators Group. It was my exposure to this group that led me to learn how the addition of a checkbox on the SAR form might prove beneficial to both SAR reporters and law enforcement. In addition, in 2011 I authored an article in *ACAMS Today* titled “\$5.00 to Ruin the Life of Children and Women: Internet Ad Sites Used to Launder Money in Promoting Prostitution/Human Trafficking.” I worked tirelessly to find suitable outlets to share the knowledge I had gathered about HT. It was during the writing of my 2011 *ACAMS Today* article that I decided that I not only wanted to educate the public about HT, but I wanted to effect real change.

AT: Is this when you started the campaign for the checkbox on the SAR form for HT/HS?

JA: Absolutely. At this point in my career, I had a firm understanding of the power of the SAR in helping law enforcement to fight financial crimes, including HT and HS. Remember, it wasn't until FinCEN released Guidance A008¹ in 2014 that specific verbiage was required in the SAR narrative, so that accurate tracking of HT and HS reports could occur. If the specific verbiage isn't added, accurate tracking of reported cases becomes near impossible. The “simple” addition of a checkbox for HT/

¹ “Guidance on Recognizing Activity that May Be Associated with Human Smuggling and Human Trafficking—Financial Red Flags,” FinCEN, September 11, 2014, <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a008>

HS will support more accurate reporting. In addition, I think it sends a clear message that the U.S. law enforcement community is committed to investigating and prosecuting HT/HS with the same intensity it does fraud, money laundering and terrorist financing. The influence of the SAR checkbox for HT/HS is solid affirmation throughout the financial services industry that we must train compliance investigators and branch associates to understand the red flag indicators for HT/HS.

AT: Was the campaign to have a checkbox added to the SAR for HT/HS an easy undertaking?

JA: Initially I thought it would be easy. I was quickly proven wrong. I came to understand that updating the SAR to include a checkbox for HT/HS would be a long battle and not a short scuffle. I presented at industry conferences and a human rights' Anti-HT Conference to raise awareness on updating the SAR for an HT checkbox. A major break in the campaign came when I received an opportunity to write for the 23rd Edition of the SAR Activity Review Trends, Tips and Issues. The publication of the article was energizing because it cemented that notion that the financial services industry could drive public policy change. The article raised an enormous amount of industry awareness to my campaign.

AT: What would you describe as the turning point in the campaign for the SAR checkbox for HT/HS?

JA: At an Anti-HT event, I had a few minutes to speak with Congressman Ted Poe (TX) about my efforts to fight HT—specifically with the update to the SAR. Thankfully, Congressman Poe understood my message and encouraged me to continue my efforts. His office put me in touch with his senior legislative representative in Washington, D.C. It took about two years for Congressman Poe to agree to author a letter to FinCEN requesting the SAR to be updated to add a checkbox for HT/HS. In 2015, Congressman Poe's office sent a letter signed by Congressman Poe and Congresswoman Carolyn B. Maloney (NY) to FinCEN requesting that the SAR be updated for HT. An excerpt of the letter states:

"The current suspicious activity categories, which include fraud, money laundering, and terrorist activity, are sensible and important, but we write today to request that the SAR also include human trafficking. As the agency's September 2014 guidance notes, financial institutions have a critical role to play in identifying and reporting transactions that may be related to human trafficking and human smuggling. Given the financial aspect of this crime, it is logical and critical to add this category. The addition will help to identify human traffickers and save victims as well as aid in the collection of much needed statistics of this widespread crime."

I thought that when Congressman Poe's letter went to FinCEN, the update would soon follow. The Congressman's letter resulted in no immediate response from FinCEN. It was only after my continued requests for the Congressman's office to follow up with FinCEN that FinCEN provided various reasons why the SAR form would not be updated.

I understand the value of accurate reporting of the horrific crimes of HT and HS; thus, I was not deterred by this setback.

While I was working with Congressman Poe's office, I was simultaneously emailing the President through Whitehouse.gov. In June 2015, a deputy at FinCEN sent an email thanking me, on behalf of the White House, for my work in fighting HT. He invited me to join a conference call with two FinCEN deputies and their subject-matter expert on HT. For 45 minutes we discussed updating the SAR to include the checkbox for HT/HS. They explained the barriers—high cost for the change and no direct request from law enforcement for the update. At the end of the call, both sides had a better understanding of the other side. The discussion did not have the result I was hoping for; however, the cause had gained a lot of notice in the highest reaches of our government. This was the turning point in the campaign—the cause was gaining recognition and being taken seriously.

AT: So, where do you turn when FinCEN declines your request for the checkbox? It seems as if FinCEN's denial would be a deal-breaker.


JA: I was not discouraged. I kept my campaign on track. I met Congressman Trey Gowdy (SC) and talked to him about updating the SAR for HT. In addition, I continued to reach out to Whitehouse.gov. I took every opportunity presented to speak with government officials about updating the SAR form. I even presented the idea to former RNC Chairman Reince Priebus during the Republican National Presidential debate.

I continued the campaign in social media with industry colleagues and the anti-HT community. I also started a Twitter campaign to members of Congress, President Trump and staff. Honestly, I have been laser-focused for the past six years on my mission for the SAR to include a checkbox for HT/HS. No stone was left unturned.

AT: Has your campaign been successful?

JA: The final result is not yet in; however, I am happy to report that on February 2, 2017, FinCEN released proposed revisions to the SAR form,² which does include the addition of a checkbox for HT/HS.

AT: Thank you for sharing your story. Any closing thoughts?

JA: I am looking forward to the day the "new" SAR form with the HT/HS checkbox is finalized and released. However, the release of the revised SAR form is not the end game. Our work as financial crime investigators in fighting HT continues. We must work together with our partners in law enforcement to raise awareness of HT and HS with the goal to eradicate this horrific crime and rescue the victims. The revised form is not the end of the campaign. It is merely the beginning of a new one. 

Interviewed by: Amy Wotapka, CAMS, BSA officer, First American Bank, Vernon Hills, IL, USA, awotapka@firstambank.com

² Federal Register, February 2, 2017, https://www.fincen.gov/sites/default/files/federal_register_notices/2017-02-08/BSAR_2017-02235.pdf

EFFECTIVELY AUDITING THE FOUR PILLARS OF THE SCREENING PROCESS

To combat money laundering and terrorist activities, financial regulatory authorities are becoming stricter on the implementation of a robust anti-money laundering/counter-terrorist financing (AML/CTF) program across financial institutions. The number of penalties and fines levied by regulatory authorities have been growing in the past few years. Thus, it is imperative that financial institutions have a robust AML/CTF program in place and that they periodically test their program since it is a regulatory requirement of Section 352 of the USA PATRIOT Act. This article covers the key sensitive areas where an effective audit focuses to ensure a strong compliance environment.

The Financial Action Task Force's (FATF) AML/CTF methodology recommendations state that "financial institutions should be required to maintain an adequately resourced and independent audit function to test compliance (including sample testing) with procedures."

This recommendation highlights the importance of performing regular audits in the compliance area for an organization. It has been observed that though many organizations and big financial institutions are continuously improving and investing in their compliance program, there are still some deficiencies and gray areas. As technology is at the core of any compliance program today, their calibration—as per the organizational need—is of utmost

importance. Many software companies are coming forward to leverage the demand of the industry, providing customized software packages to perform watch-list filtering, which is the heart of any AML program. The basic functionality of these packages revolves around their data matching technologies, which they accomplish through fuzzy logic algorithms. Regular tuning of these packages is required to reduce the number of false positives. In addition, proper documentation and data archival procedures have to be adopted for look-back purposes.

The key sensitive areas that should be covered in the audit of a compliance program to ensure its robustness and efficiency, are listed next.

Review of internal and external data feeds

The concept of GIGO (garbage in, garbage out) can be applied to any software package deployed as part of a screening solution. Its efficiency is governed by the quality of data entering into the system. We can classify the data used in a screening solution in two parts:

- The list of sanctions, politically exposed persons (PEPs), special interest persons (SIP) and relatives of close associates (RCA), which are updated and published on a regular basis by organizations like the Office of Foreign Assets Control. These lists are used as a reference point and matched against customer data.
- The customer/entity data of the organization has to be screened against these lists to ensure that the financial institution follows the prescribed approach toward them. For example, the financial institution must not entertain sanctions in any way as they are linked to terrorist activities and high degree crimes. Similarly, PEPs must be subjected to enhanced due diligence.

If the data feeds contain data quality issues (e.g., the names are mentioned in single letters, or there are missing fields), then it would directly affect the efficiency of the screening process. This would

create a large number of false positives, which would lead to a waste in both time and resources in the investigation.

Review of screening solution

The second pillar of the screening process is the screening solution deployed by an organization. This is the area where the actual screening occurs and the potential risks are notified. The data coming from both ends are matched to check the potential sanctions, PEPs, SIP and RCA. It has its own fuzzy logic algorithms to match the data and if that match goes beyond a certain threshold then it generates an alert. So, different data fields have different weights in contributing to an alert. As the whole mechanism of this solution revolves around the name matching technology, its efficiency is also governed by the accuracy with which it is performed. So, what adds to its complexity? The data related to people, organizations and countries are coming from different parts of the world and hence from different cultures, in different languages and different nomenclatures. This in itself makes the matching process a bit challenging. Hence, these inefficiencies in the screening solution can result in false positives and false negatives.

False positives are alerts that are generated from matches that are not genuine. Even though these customers were falsely matched and they do not actually fall into any of the risk categories and are clean, the alerts were still generated. This causes a waste in money, time and resources. The whole calibration of the screening program is focused on reducing this number.

False negatives are the opposite of false positives and could be even more dangerous. It is like a criminal escaping the security process. The false positives not only lead to a waste in resources, but they could have a critical impact in terms of legal, reputational and financial losses.

The screening process requires regular tuning to maintain the trade-off between the two. The screening should not be too strict where false positives are generated and genuine customers are

negatively impacted. Similarly, they should not be too lenient where it could lead to criminals escaping.

Periodic auditing of the internal configurations and the alert generation process of the screening solution is required to check its effectiveness. The hits that are getting generated should be analyzed whether they are in line with the screening requirements.

To accomplish this, the screening review process should be reviewed in terms of historical alerts and predefined codes. The evaluation should also include the review of its threshold tuning—whether that is being periodically orchestrated commensurate with this dynamic environment.

The quality of documentation around the periodic updates and around potential issues is critical. One cannot disparage the importance of documentation in the compliance world. It is one of the most important parameters over which an institution's sincerity toward its program is gauged. It not only smooths the audit process, but it also plays a great role in tracking the performance of the entire compliance system.

The list management of the screening solution should be thoroughly reviewed to ensure that it is consistent with the documented policies (e.g., if the policy around PEPs says, “former PEPs should be considered live PEPs,” then it should also be reflected in their list configurations).

An effective screening system cannot be accomplished without a meticulous alert handling management system with well-defined procedures. The process—especially the rationales behind disregarding alerts—should be well evidenced and documented.

Review of relevant policies and procedures

The policies and procedures deployed by a financial institution have to be reviewed against regulatory policies. This should be conducted by using the assessment tools and by interviewing and following-up with relevant personnel. Questions that could be asked are


what course of action is employed in case of a confirmed sanctions match? When should a suspicious activity report be filed?

Review of governance and oversight arrangement

Ensure that all relevant stakeholders are well updated and that lines of communication to all stakeholders is clear by reviewing the responsibility assignment (RACI) matrix. The change management process should be well defined and should fully identify, assess and document the impact of the changes. The review should include meetings with representatives from first, second and third lines of defense including, AML Key Control Function (KCF), IT services and group security, business compliance oversight, business transformation and retail strategy to ensure a detailed RACI matrix and to clearly define the roles and responsibilities within the screening framework.

The independent reviewer involved in the audit process should perform the comparative analysis in the key areas mentioned above, among peers, with similar distribution lines and products that face equivalent threats. Auditing must be in compliance with the legal and regulatory requirements that apply to customer screening.

Conclusion

Achieving ideality in this complex and evolving compliance environment may not be possible, we must still strive toward perfection by ensuring that our compliance system is commensurate with this ever-changing environment. The best way to accomplish this is to have a well-organized periodic auditing system in place. Many financial organizations procrastinate on this front and avoid investing in self-organized third-party auditing, but they need to understand that a stitch in time could save nine. 

Abhinav Kaushik, CAMS, AML consultant, Infosys, Swindon, U.K., abhinav_kaushik@infosys.com



FROM LAW ENFORCEMENT TO AML AND FRAUD COMPLIANCE

Editorial credit: Andriy Blokhin/Shutterstock.com

Throughout my career, I have been blessed to be associated with many outstanding and dedicated professionals. My post-college work experience in the public and private sectors has now spanned the better part of 45 years. I served in the U.S. government for 31 years before moving into the business world, where I have been employed for the last 14 years. I had the honor of starting my career as a revenue agent in the Internal Revenue Service. My ambition since the age of 12 was to become a special agent in the Federal Bureau of Investigation (FBI). That opportunity came to fruition, and I had the distinct privilege of serving in law enforcement with the FBI for 28 years. It was a fabulous experience that I will always treasure.

Where did the years go? How did they go by so fast? I can vividly remember the day I was sworn in as a new agent. I was a very excited 24-year-old with a fresh haircut, a new beige colored suit and new cordovan dress shoes. When that day came, the furthest thing from my mind was the thought of retiring from the FBI. After all, my entire career was in front of me on that day. That day, and 28 years, seemingly passed in a heartbeat. As my law enforcement career came and went, it was a great ride, with incredible memories and great stories.

With my law enforcement bias, could there possibly be life after the FBI? I cherish the fact that the answer is a resounding “Yes!” What I have come to appreciate is that my career today, as a

consultant in the anti-money laundering (AML) world, is every bit as satisfying as my law enforcement career was, but from a different perspective. I still experience a sense of accomplishment that I find quite rewarding. It is important to be able to place accomplishment in context. What I accomplished in law enforcement and what I accomplish as an AML consultant are inherently different yet similarly meaningful in providing self-satisfaction.

As with many life experiences, my post-law enforcement career started as a work in progress that left me unfulfilled and second guessing my decision to leave the FBI when I did. Retirement from law enforcement was inevitable. Even though older law enforcement

professionals possess extensive experience and situational maturity, the prevailing thought of administrators is that law enforcement is a younger person's profession. In my case, I always thought I would retire from the FBI at the mandatory retirement age. To my surprise, I retired five years before my mandatory retirement age.

I was recruited by a “headhunter” representing a Fortune 200 company to start a centralized anti-fraud program in accordance with the Sarbanes-Oxley (SOX) anti-corporate accounting fraud legislation. After some agonizing consideration, I accepted the position. Although I was well compensated and company personnel were great to deal with, I was out of place and lacked a sense of

mission or purpose. For a global holding company, I was the only former law enforcement executive. That was a real culture shock for me. More importantly, the company honestly believed they did not have a fraud problem and only wanted to implement provisions SOX mandated as necessary and no more. I was not comfortable with that type of tone. I lasted 11 months before resigning. During that timeframe, I was miserable and did a lot of soul-searching.

Part of my problem was missing the FBI and feeling regret about leaving when I did. Another part of the problem was that I missed working financial-related crimes with a money laundering nexus. One of the highlights of my career at the Bureau was working financial crimes and money laundering in close partnerships with the financial services industry, especially with bank investigators. I quickly realized that I did not adequately think through retirement from the FBI. More importantly, where could I experience a sense of meaningful accomplishment and satisfaction again? In my case, that sense of accomplishment and satisfaction comes from providing consulting services, including training, to the financial services industry regarding financial crimes, money laundering and terrorist financing.

The purpose for sharing my personal experience is to encourage current law enforcement colleagues nearing retirement age not to make the same mistake I and many others made by not being prepared and not thinking through where we would find meaningful satisfaction in our post-law enforcement lives. There is an old saying that one of my early FBI supervisors frequently repeated: "Do as I say and not as I do." I have reinterpreted that statement through the years. During training and mentoring I use the analogy, "If I knew then what I know now, I would have been dangerous" (better stated, I would have been more successful and satisfied).

Law enforcement experience affords post-diverse career opportunities in many fields. One field in particular that possesses diverse opportunities is AML and fraud compliance. One of the things I am proudest of throughout my entire career has been serving as a mentor and

sharing my experiences to help inform career development decisions by my younger peers. Based on my personal experience, transitioning from law enforcement to AML and fraud compliance is much easier than transitioning into other career paths. The reasoning for this is centered on select core values, coupled with investigative experience.

The most notable core values are sense of family and dedication. In the FBI, and in most law enforcement agencies, there is a tremendous sense of family and camaraderie. As I embarked on my FBI career, my closest friends became my FBI peers. We truly bonded as a family. Very strikingly, as my AML career has evolved, my closest friends are in the AML community. I consider them family just as I did with my FBI brothers and sisters. When I was in the FBI, I did not think anyone was more dedicated and committed to their mission than the FBI and more broadly, law enforcement. What makes the AML and fraud compliance profession so desirable is that AML professionals share the same sense of dedication and commitment. The difference between the two is context. The main similarities between the two are passion and intensity.

From the time I was a young FBI agent in New York, I have consistently witnessed a steady migration of former law enforcement personnel into the AML and fraud compliance profession. The investigative skillsets of law enforcement officers serve them well in the AML and fraud compliance space. In addition, there is incredible diversity and opportunity in the AML and fraud compliance field. Opportunities abound with financial institutions, consulting firms, vendors and as sole proprietors. Factor in the magnitude of the industry and range of institutional sizes from very small to extremely large. I am an optimist and I believe a niche can be found for all of us.

When I mentor members of law enforcement considering career opportunities in AML and fraud compliance, I encourage them to take a broad look at the industry and contemplate where their niche should be. Is it working directly for a financial institution or as a consultant providing services to financial

institutions? Once I encourage the potential law enforcement retiree to consider the diverse employment possibilities, I immediately advise them to join ACAMS, if they are not already a member. I also recommend they obtain their CAMS certification.

Invariably, I will provide a potential law enforcement retiree with guidance about their qualifications and how to distinguish themselves to stand out when opportunities arise. I believe you have to gain visibility in the industry. Visibility is built upon your reputation and through networking. Many individuals coming out of law enforcement have distinguished themselves in various ways as investigators. Those investigative skills are extremely valuable. Coupling those skills with the CAMS certification will serve to enhance one's reputation. Likewise, in my experience, many outstanding investigators possess excellent liaison skills. Those liaison skills are essential ingredients for networking. I encourage current law enforcement members to get involved with networks of retired law enforcement personnel. I also encourage them to become active members of ACAMS through participation in ACAMS chapters and events. ACAMS participation greatly enhances networking opportunities.

It is hard to believe that 45 years have come and gone in my professional career. These 45 years have provided me with a wealth of experience and have given me maturity and stability. I look forward to sharing my experience with anyone who can benefit from it. One of the things I am heartened by is the true quality in terms of integrity and competence of those individuals transitioning from law enforcement and starting new careers in AML and fraud compliance. I hope they experience the same sense of accomplishment I continue to enjoy. Likewise, I hope they establish the lasting friendships that I have been blessed to develop in the AML community. 

Dennis M. Lormel, CAMS, internationally recognized CTF expert, president & CEO, DML Associates LLC, Lansdowne, VA, USA, dlormel@dmlassocllc.com

Interviewing tips for non-IT financial crimes professionals



You have created a stellar resume by using the tips provided in the article titled “Resume Tips for the AML Professional”¹ and you have followed that up with a proactive marketing strategy as recommended in the article “Marketing 101: How an AML Professional can Increase Marketability.”² Your dedicated efforts have resulted in an interview for a non-IT related financial crimes professional role. Assuming that you have the job locked up solely because the company called you is likely the most damaging mistake you can make while job hunting. Careful preparation, from the time you get the call for the interview through the time you exit the interview, is what will set you apart from other candidates.

Upon receiving a call for an interview, your first step is to re-familiarize yourself with the company. You have already completed some research on the company when deciding whether you should apply. Now is the time to take the research to the next level:

- Research the corporate structure, locations, asset size and the number of branches (if applicable).
- Get a sense of their business model and products/services offered.
- Understand what federal and/or state examinations the company is subject to.
- Learn what you can about the company's culture from news articles or by reaching out to peers on social networking sites.
- Determine if the company is under a consent order (Note: Do not bring the topic up unless the interviewer mentions it first).
- “Analyze the job description and your match with it. Write out their requirements and how you meet those requirements.”³ Your goal in the interview is to stand out, in a good way, among the other candidates. Hubris/ego needs to be in check when speaking about your qualifications for the role. As you did when crafting

your resume, be honest! Do not oversell your qualifications or you may find yourself in a role for which you are unprepared. Speak honestly about your experience with various technology and systems, audits and examinations.

- Find ways to “convey that you want the position and would be motivated to excel in the role long-term. If you're only interviewing for this job because you need the paycheck, that's going to come through.”⁴ Asking about opportunities for advancement within the organization can also lead a recruiter or hiring manager to think you may be in the role short term, so tread lightly here.
- Do not assume the interviewer knows your background or your accomplishments. Remember that oftentimes employers review your resume for less than a minute. Be prepared to demonstrate how you will be of value to the organization or the team. Have examples of when you took initiative and made a positive impact in your current or former roles (Note: be careful not to disclose confidential or proprietary information).
- Beware of terminology overload—especially if the interviewer is from human resources and is not the hiring

manager. The interview is certainly the right time to display knowledge, but continuous name-dropping of software and applications may get tiresome for the non-subject matter expert interviewer, resulting in a negative impression.

Prepare for common interview questions like “Where do you see yourself in five years?” In addition, when answering the question “Why are you leaving your current role?” follow the tips below:

- Avoid making negative comments about current/prior employers. Negativity breeds negativity. It may leave the interviewer wondering what you will be saying about his/her organization when you leave there.
- Give serious consideration when formulating your response. A simple internet search will result in pages of links purporting how to best answer standard interview questions.
- Practice your responses in front of mirrors, friends or a mentor. Replace the word “can” in your responses with the word “have.” For example, say “I have led a team of experienced suspicious activity monitoring investigators” in lieu of “I can lead a team of experienced suspicious activity monitoring investigators.”

¹ Amy Wotapka, “Resume Tips for the AML Professional, *ACAMS Today*, December 2016-February 2017, <http://www.acamstoday.org/resume-tips-for-the-aml-professional/>

² Amy Wotapka, “Marketing 101: How an AML Professional can Increase Marketability,” *ACAMS Today*, March-May 2017, <http://www.acamstoday.org/marketing-101-how-an-aml-professional-can-increase-marketability/>

³ Susan P. Joyce, “The 10 Deadly Job Interview Mistakes (and How to Avoid Them),” *Job-Hunt*, https://www.job-hunt.org/job_interviews/avoid-interview-mistakes.shtml

⁴ Pamela Skillings, “Recruiters Reveal: Top 10 Reasons You Didn't Get the Job,” *Big Interview*, April 28, 2016, <https://biginterview.com/blog/2016/04/job-interview-feedback.html>

- “Canned” responses will not win points with an interviewer, so ensure your responses are genuine. In addition, if you take too long during the interview to formulate a response, it may appear as if you are being untruthful.
- Golden rule when interviewing: above all else, be honest.

Prepare for uncommon interview questions like:

- Can you give me the names of four people whose careers you have fundamentally improved?⁵
- How do you handle criticism?
- What is your management style or what management style do you work best under?
- Do you prefer being a sole contributor or working on a team?

The most difficult interview question to answer is concerning salary expectations. “Before you consider answering the question, it is important to know the going rate for jobs in your field and in your job market (location). These can be found on web-sites like payscale.com, glassdoor.com and salary.com.”⁶

Bankrate.com⁷ cost of living comparison will provide valuable information on cost differences for living expenses between two cities if relocation is being considered. Also, be aware of the term “all in” meaning the figure you are quoting includes bonuses. Be very specific about relocation expense expectations or other costs you may want the organization to incur such as supporting your CAMS membership (annual dues and recertification credit needs).

Even though the day of the interview has arrived and you have been preparing for this opportunity to showcase your qualification for weeks, there is still more prep work to be done:

- Ensure that your appearance conveys exactly what you intend. Clothes should not be wrinkled. Use cologne or perfume sparingly. Do not chew gum; however, a breath mint before walking in might be advisable. Comb your hair and check for stray hair(s) on your clothes.
- If the interview is by Skype, FaceTime or otherwise not in person, ensure that there is little to no background noise to interfere with conversations. If using Skype, etc., ensure that you select a location that has a suitable background (lying on your bed for the call is not acceptable).
- Check a mirror before the interview. Ladies, if wearing makeup, ensure it is well-applied with no streaks. Men should check zippers. Both women and men should ensure that there is no food lingering in teeth. You want the interviewer completely focused on you and not a spot on your shirt or spinach in your teeth.
- Arrival time matters. Never be late to an interview. Being too early is also dangerous. Strive to arrive no more than 10 to 15 minutes prior to the interview start time. Ensure you allow time for traffic backups or other unforeseen delays.

During the interview:

- Walk in with confidence. Have a strong handshake and a big smile. Your body language must convey confidence. “Good posture, smiling when appropriate, making eye contact and leaning forward are all positive ways to express your interest in the job.”⁸

- Display solid interpersonal skills. Use humor appropriately. Giggles may display nervousness. Be an “active listener.” “Active listening involves listening with all senses. As well as giving full attention to the speaker, it is important that the ‘active listener’ is also ‘seen’ to be listening—otherwise the speaker may conclude that what they are talking about is uninteresting to the listener.”⁹
- Turn off your cell phone. Do not set it to vibrate—turn it off! You want your full concentration to be on the interviewer and the questions. In addition, you want the interviewer’s full attention on you and not the annoying vibrations emanating from your phone.
- Highlight industry certifications like CAMS, CAMS-FCI and CAMS-Audit. Regulators appreciate when an institution makes the effort to develop a well-qualified staff. Walking into the job with one or more industry certifications is a positive differentiator for an applicant. Likewise, if you have experience in interviewing suspects, testifying in court, law enforcement or any other sought-after skill; find at least one opportunity to mention it in the interview.
- Illustrate your commitment to the industry and the role by mentioning industry events that you have attended, arranged, presented at, etc. If you are on the board of a local ACAMS chapter or you are an active participant in an ACAMS task force, be certain to highlight how the activity will benefit the company with which you are interviewing.
- Find ways to work into the conversation that you are “fungible” by focusing on transferrable skills. Experience in people management and project management are skills that can

⁵ Betsy Mikel, “How You Answer This Interview Question Reveals Your True Character,” *Inc.*, January 4, 2017, <http://www.inc.com/betsy-mikel/1-interview-question-that-cuts-through-the-bs-to-reveal-someones-true-character.html>

⁶ Pamela Skillings, “How to Answer: What Are Your Salary Expectations?,” *Big Interview*, October 25, 2015, <https://biginterview.com/blog/2015/10/salary-expectations.html>

⁷ Cost of Living Calculator, Bankrate, <http://www.bankrate.com/calculators/savings/moving-cost-of-living-calculator.aspx>

⁸ Pamela Skillings, “Recruiters Reveal: Top 10 Reasons You Didn’t Get the Job,” *Big Interview*, April 28, 2016, <https://biginterview.com/blog/2016/04/job-interview-feedback.html>

⁹ “Active Listening,” *Skills You Need*, <http://www.skillsyouneed.com/ips/active-listening.html>

“
The more
effort you put
in before the
interview, the
more likely
you are to be
successful
during the
interview”



be used in many different types of roles within the organization. When an applicant can participate in many parts of the organization's AML program, it is a win for the company. Clearly demonstrate that you are able and willing to assist with not only the role applied for, but also other areas of the program.


Close out the interview with the same level of confidence you walked in with. Your goal in closing out the interview is to get a good sense of where you stand in the hiring process.

- Questions like the following¹⁰ will help you gauge how the interview went:
 - ♦ “Based on my background and the skills and experience we discussed, how well do I fit the profile of the candidate for which you’re looking?” or
 - ♦ “Given what we’ve just discussed during this interview, do you have any concerns about my fit for this position?”
- “Ask what the next steps in their hiring process are if no one volunteers the information.”¹¹ This question will demonstrate to the interviewer your desire to move forward with the application process.
- Remember to thank the interviewer for his/her time and the opportunity to discuss how you will be an asset to the company.

Finally, after the interview follow up with the interviewer. Via email (not phone) thank the interviewer, again, for his/her time. Keep the email short and to the point. Demonstrate your interest but not desperation.¹²

Be on the lookout for signs from the interviewer that you are no longer being considered for the role:^{13,14}

- A clear timetable for next steps was not provided.
- It was stated during the interview that you are overqualified.
- The interviewer politely notified you that they are still looking at other candidates.
- The interviewer provides helpful but unsolicited advice regarding your resume, career or interviewing skills.
- The interviewer wishes you luck on your job search as you are walking out the door.
- The job was reposted after your interview.
- They have not responded to your follow-up email.

While a job interview can be nerve-racking, it does not have to be. To reduce the stress that often accompanies an interview appointment—create a plan to succeed. Mastering a job interview takes preparation and practice. The more effort you put in before the interview, the more likely you are to be successful during the interview. Remember, preparation is the key to a successful interview experience. 

*Amy Wotapka, CAMS, BSA officer, First American Bank, Vernon Hills, IL, USA,
awotapka@firstambank.com*

¹⁰ Lisa Quast, “Job Seekers: How to Close an Interview with Class,” *Forbes*, March 17, 2014, <http://www.forbes.com/sites/lisaquast/2014/03/17/job-seekers-how-to-close-an-interview-with-class/#5c4db86e6907>

¹¹ Susan P. Joyce, “The 10 Deadly Job Interview Mistakes (and How to Avoid Them),” *Job-Hunt*, https://www.job-hunt.org/Job_interviews/avoid-interview-mistakes.shtml

¹² Yolanda Owens, “3 Rules for Following Up With a Recruiter,” *The Muse*, <https://www.themuse.com/advice/3-rules-for-following-up-with-a-recruiter>

¹³ John Egan, “13 Telltale Signs that You Didn’t Get the Job,” *Huffington Post*, April 28, 2014, http://www.huffingtonpost.com/john-egan/13-telltale-signs-that-you_b_5199895.html

¹⁴ Raven Ishak, “9 Signs You’re Probably Not Getting the Job,” *Bustle*, August 19, 2016, <https://www.bustle.com/articles/178366-9-signs-youre-probably-not-getting-the-job>

WHITE-COLLAR CRIME:

The carousel of VAT abuse

Value-added tax (VAT) is one of the most critical sources of national revenue by the majority of European state authorities, particularly in the Central and Eastern European (CEE) region. It is basically a consumption tax calculated on the value added to goods and services. It is levied on almost all commercial activities inclusive of the manufacturing and distribution of goods and the provision of services that are purchased and sold across the European Union (EU). Therefore, in order to create the environment for fair trade competition, products/services exported outside of the EU are VAT-free, whereas imported ones are subject to taxation.¹

Considering the VAT's significance to the fiscal well-being of states, declining to pay it may contribute to considerable deficiency in the delivery of public services and thwart fair market practices, because it generates higher tax obligations on honest taxpayers.² This observation is consistent with the 2010 findings presented by Richard Murphy, a chartered accountant and a political economist, who carried out a research project at the request of Tax Justice Network. He analyzed data from the World Bank, CIA World Factbook, Heritage Foundation and the World Health Organization. He estimated that the financial revenue losses worldwide, generated as a direct consequence of tax abuses, equaled to approximately \$3.1 trillion and represented 98 percent of global GDP.³ Unequivocally, VAT fraud has paramount consequences on the proper functioning not only of the global economy, but also of the EU Single Market. In

accordance with the European Commission's findings from 2013, VAT evasion affects approximately 18 percent of the total VAT base across the Union.⁴ Europol estimates that 40 to 60 billion euro of the yearly VAT revenue losses of EU states result from actions of organized crime groups and that 2 percent of those groups are behind 80 percent of the missing trader intracommunity fraud.⁵ The 2016 report on tax matters presented by PWC established that the VAT gap (i.e., the difference between the VAT, which should be collected and the actual tax revenues) oscillated between 19.1 percent in the Czech Republic to just under 40 percent in Romania. Considerable VAT gaps were also identified in Hungary (20.8 percent), Slovakia (28.3 percent) and Poland (29.2 percent). The report estimated the unremitted VAT in 2014 and 2015 amounted to 3.1 billion euros in Czech Republic, 2.6 billion euros in

Hungary, 8.3 billion euros in Romania, 12 billion euros in Poland and 2.2 billion euros in Slovenia.⁶

VAT charges within the EU

Overall, VAT avoidance could take place in any transnational trade flow. Individual importers are subject to customs duties and VAT on imports at the destination border. Therefore, in instances where tariffs are not due (e.g., in the presence of a free trade agreement between states or where there is a customs union between states, such as the EU) those engaged in importing goods/services are enticed to misrepresent their trade numbers so as not to pay VAT dues.

Indeed, the EU as a single market constitutes a unique inducement for tax fraudsters due to the ease with which products and services are transferred across its borders. The current transitional VAT regime encompasses the

¹ European Commission, "What is VAT?," accessed February 28, 2017, http://ec.europa.eu/taxation_customs/business/vat/what-is-vat_en

² Katerina Gradeva, "VAT Fraud in Intra-EU Trade," August 7, 2014, <http://www.etsg.org/ETSG2014/Papers/378.pdf>

³ F. Schneider, Konrad Raczkowski, and Bogdan Mróz, "Shadow economy and tax evasion in the EU," 2015, 18 Journal of Money Laundering Control 34, 41.

⁴ Katerina Gradeva, "VAT Fraud in Intra-EU Trade," August 7, 2014, <http://www.etsg.org/ETSG2014/Papers/378.pdf>

⁵ European Court of Auditors, "Tackling intra-Community VAT fraud: More action needed," 2015, Special Report http://www.eca.europa.eu/Lists/ECADocuments/SR15_24/SR_VAT_FRAUD_EN.pdf

⁶ Ulrika Lomas, "Central, Eastern European VAT Gap At EUR28bn," Tax-News, June 27, 2016, http://www.tax-news.com/news/Central_Eastern_European_VAT_Gap_At_EUR28bn___71557.html



destination principle for taxation purposes, and it is applicable to trade flows across the member states. In essence, all trade conducted within the EU borders is exempt from VAT obligations, as the importing party obtains products and services VAT-free from the exporting counterparty. Subsequently, the VAT is charged when goods are sold to customers, and the tax is then submitted to the national tax authorities. According to Katerina Gradeva, “the transitional regime breaks the VAT chain at a very vulnerable stage; all intra-EU trade flows are transported VAT-free, which leaves potential for massive VAT fraud.”⁷

The ins and outs of VAT fraud schemes

Tax authorities across the EU and the CEE region in particular exhibit gross inaptitude in employing effective strategies to prevent and fight VAT-related abuses. Since the EU guarantees the free movement of goods, capital, services and people, it becomes exceptionally challenging to control intra-community trade, especially in relation to the following commodities: cell phones, integrated circuits (predominantly micro-processors and chips), natural gas and electric power certificates, telecommunications services, raw metals or semi-processed elements of metals, game controls, laptops, tablets, and cereals and industrial crops.⁸ The selection of these particular goods is not random, as they serve well in the perpetration of one of the most ubiquitously employed VAT fraud schemes, the VAT carousel fraud, also known as missing trader intra-community VAT fraud. Through carousel fraud, perpetrators engage in the importation of goods where they do not merely underreport the adequate value of the imports, but the involved business vanishes into thin air without remitting any VAT to the national tax administration (hence, the missing trader) once the sales are concluded. In addition, VAT fraud could be conducted through various other conduits, such as, according to Gradeva, the “underreported sales (‘off the books’ sales), no firm registration to the tax authorities (‘ghost’ firms), misclassification of products in the case when a firm sells several goods taxed at

different VAT rates, false claims for credit based on overstated VAT paid on inputs and imported products which are not brought into tax.”⁹

One of the most prominent cases of the VAT exploitation within the EU

Operation VERTIGO began on March 3, 2015, and it is one of the most prominent cases of VAT fraud across the member states. It literally traversed the EU and was investigated by authorities from the Czech Republic, Germany, the Netherlands, and Poland, with Spain, the U.K., Belgium, Cyprus, Denmark, Ireland, Luxembourg, Gibraltar, Ukraine, Eurojust and Europol also involved. VAT evasion and illegal VAT non-reimbursements equalled more than 100 million euros in Germany, approximately 30 million euros in the Netherlands, and 10 million euros in the Czech Republic and Poland respectively. In short, the investigation started when Dutch and German officials noted a high volume of VAT returns from a number of businesses that engaged in carousel fraud practices.

⁷ Katerina Gradeva, “VAT Fraud in Intra-EU Trade,” August 7, 2014, <http://www.etsg.org/ETSG2014/Papers/378.pdf>

⁸ F. Schneider, Konrad Raczkowski, and Bogdan Mróz, “Shadow economy and tax evasion in the EU,” 2015, 18 *Journal of Money Laundering Control* 34, 41.

⁹ Katerina Gradeva, “VAT Fraud in Intra-EU Trade,” August 7, 2014, <http://www.etsg.org/ETSG2014/Papers/378.pdf>

The joint investigation team managed to establish that certain goods and commodities were in theory forwarded to the targeted country for alleged onward consumption, but instead they were sold via numerous business establishments within the targeted country and subsequently shipped, resulting in an illegal reimbursement from tax authorities. The fraudsters utilized alternative banking platforms worldwide to, as stated by Europol, “facilitate crime-related money transfers and associated money laundering,” oscillating around several hundred million euros.¹⁰

The way forward at the pan-European and the state level within the CEE region

With the benefit of hindsight, these examples demonstrate the general understanding among public officials and the law enforcement community that organized criminal networks are far from ceasing their illegal activities, particularly when it comes to VAT abuses. Back in 2007, BDO Stoy Hayward, an accounting firm, observed that “Sadly, crime does often pay at the moment if you are a fraudster, which explains why large frauds are on the increase.” Although there was a clampdown on such activities, the skepticism about halting “this avalanche of huge frauds against the taxpayer” remains.¹¹ Indeed, it seems that criminals may virtually use any commodity to engage in VAT fraud schemes, thus depriving state authorities of millions of euros. Therefore, one of the most pressing and simultaneously the most challenging issues for the EU as a whole and its individual members is the matter of tightening the VAT tax systems and introducing effective countermeasures to discourage potential criminals from engaging in VAT-related extortions.

EU’s efforts in combating VAT fraud

The EU’s policy agenda has focused on the member states’ tax regimes for a couple of years. The general challenge is “a relative lack of convergence” across states, and that each country is following its own agenda to tackle tax policies, particularly VAT.¹² The EU addressed the issue of tax-related crimes already in 2006 with the implementation of Council Directive 2006/112 EC on a common system of VAT. This document essentially restrained, to a certain extent, VAT extortion for scrap metal. It was subsequently amended in 2010 with the Council Directive 2010/23/EU and the Council Directive 2013/43/EU. That latest piece of EU legislation focused on tax matters by transferring the obligation to settle VAT from the supplier (as typically mandated under the EU law) to the end customer for whom the given service was performed or a commodity delivered. This changed VAT into a reverse charge mechanism, as it reversed the liability for the payment of VAT.¹³ The objective behind this measure is to significantly reduce, if not eliminate, carousel schemes altogether. According to the directive’s provisions, individual states will be at liberty to enforce the new directive temporarily within the following

sectors: “mobile phones, integrated circuit devices, gas and electricity, telecoms services, game consoles, tablet PCs and laptops, cereals and industrial crops, and raw and semi-finished metals.”¹⁴ The directive facilitated the application of the reverse charge principle for a maximum of two years until the end of 2018.¹⁵ Alongside the reverse charge mechanism, in 2012, the EU proposed the implementation of a quick reaction mechanism (QRM) that essentially facilitates an instantaneous response to a potential carousel fraud or any exorbitant VAT fraud. The affected member state has emergency powers that it could apply to immediately address VAT extortions, provided the EU Commission has been notified 30 days in advance. With the employment of the QRM, there will be an expedited process in place to enforce a reverse charge to particular provisions of goods and services for a limited time period until December 31, 2018.^{16,17}

These legislative efforts were further supported by the establishment of Eurofisc in 2010, which was to act as a decentralized cooperation network for VAT. Nonetheless, it turned out to be a very obscure and ineffective system of information exchange.¹⁸ As evidenced by the latest international VAT fraud scandals, the EU has a long way to go to deliver an effective strategy for combating VAT extortion. Though, in fairness, it has to be acknowledged that the EU does recognize the necessity to reduce the tax gap (to at least by half by 2020), tax fraud, and tax evasion (Fiscalis 2020 program).¹⁹

¹⁰ Europol, “Major Europe-Wide VAT Fraud Network Busted with the Support of Europol and Eurojust,” March 3, 2015, <https://www.europol.europa.eu/newsroom/news/major-europe-wide-vat-fraud-network-busted-support-of-europol-and-eurojust>

¹¹ Andrew Taylor, “Carousel fraud defies new law,” *Financial Times*, August 13, 2007, http://www.ft.com/cms/s/0/78e02a0c-4935-11dc-b326-0000779fd2ac.html?ft_site=falcon&desktop=true

¹² Mazars, “Mazars Central Eastern European Tax Guide 2016,” http://www.taxlink.lv/f/Mazars%20CEE%20Tax%20Guide_2016_web_small.pdf

¹³ F. Schneider, Konrad Raczkowski, and Bogdan Mróz, “Shadow economy and tax evasion in the EU,” 2015, 18 *Journal of Money Laundering Control* 34, 41.

¹⁴ Michael Hennigan, “European Union continuing to struggle in fight to reduce VAT fraud,” *Finfacts*, September 3, 2013, http://www.finfacts.ie/irishfinancenews/article_1026481.shtml

¹⁵ F. Schneider, Konrad Raczkowski, and Bogdan Mróz, “Shadow economy and tax evasion in the EU,” 2015, 18 *Journal of Money Laundering Control* 34, 41.

¹⁶ European Commission, “VAT: Commission proposes new instrument for speedy response to fraud,” July 31, 2012, http://europa.eu/rapid/press-release_IP-12-868_en.htm

¹⁷ Michael Hennigan, “European Union continuing to struggle in fight to reduce VAT fraud,” *Finfacts*, September 3, 2013, http://www.finfacts.ie/irishfinancenews/article_1026481.shtml

¹⁸ F. Schneider, Konrad Raczkowski, and Bogdan Mróz, “Shadow economy and tax evasion in the EU,” 2015, 18 *Journal of Money Laundering Control* 34, 41.

¹⁹ *Ibid.*

However, tax evasion is not a national or even European domain, but it is a transnational concern that is being addressed by a multitude of international organizations. These include the OECD, which adopted an action plan for combating tax base erosion and profit shifting in 2014 with guidance on transfer pricing documentation and country-by-country reporting.²⁰

State efforts in combating VAT fraud

Unequivocally, the EU and international initiatives aimed at effectively tackling the issue of VAT tax abuse are commendable, though little can be achieved without individual states employing comprehensive and effective countermeasures of their own. In spite of comparatively low income tax duties, the tax-levying efficacy across the CEE region has been quite inefficient. State authorities have concentrated on reducing the “VAT gap—the residual between actual VAT revenues and hypothetical VAT revenues derived from the gross value added created in the economy.”²¹

Since there is no unified approach across the member states toward handling VAT matters, each state is basically at liberty to embrace and implement virtually any anti-abuse VAT initiatives they deem adequate within their jurisdictional perimeter. Hence, the following measures have recently been or will be enforced in some EU states:


- Electronic cash registers—The enforcement of the measure has been quite appealing to many EU states; nonetheless, the primary focus is on tax evasion within the retail industry rather than cross-jurisdictional VAT fraud schemes

- Online cash registers and electronic reporting systems—Ukraine embraced the electronic VAT administration system, whereas the issuing of VAT invoices has an amount cap. To obtain VAT reimbursement, a taxpayer is obliged to get a VAT-invoice in electronic format, which is recorded with the Unified Register of VAT invoices, from the seller/supplier. Then, the VAT credit is received under two registers with a chronological order of payment. Bulgaria, Croatia, Hungary and the Czech Republic adopted similar measures
- Further implementation of the reverse charge mechanism for VAT across the CEE region²²
- Enhancing transfer pricing rules²³
- Online registration of the international transportation of products (Hungary)²⁴
- Establishing a database of invoices issued by taxpayers accessible to the tax authorities. The proposed measure involves the uploading of invoices into the database in real time. Certain legal and technical impediments are unavoidable, such as the issuing of electronic versus paper form invoices. For the system to work, only the electronic invoices should be deemed legitimate, and EU law would have to be amended accordingly to reflect that change. The matter of adequately trained tax resources on the part of the tax authorities and prompt and accurate processing of the data are also challenges. The database could become a powerful tool in fighting VAT abuses²⁵
- VAT control statements—The measure was swiftly embraced by Slovakia and the Czech Republic. In short, these reports would be submitted every month, with the

information on invoices issued and obtained by the VAT-registered taxpayer with details such as the number of the invoice, VAT amount, VAT base and tax point. If the information submitted by the vendor and the purchaser differ, then authorities are instantaneously notified (the Czech Republic)²⁶

- The split payment mechanism—In short, the state officials name a third party (be it a public body or a financial institution) to levy instantaneously output VAT. The purchaser would then settle the net price with the supplier and transfer the VAT to that third party. As a result, the latter is no longer under the obligation to settle their output tax (Italy)²⁷
- Lotteries to ensure that all transactions are recorded (Poland)²⁸

Conclusion

Unequivocally, combating effectively VAT fraud is a battle that each Member State, but more importantly the EU, as a whole needs to fight. The pertinent legislative framework, as well as the administrative cooperation in intra-community trade, reflects well on the EU's efforts to address tax abuses. Nevertheless, as the data shows, an effective implementation and execution of the countermeasures to tackle the VAT exploitation still requires effort and commitment on the part of the governments, tax authorities as well as the law enforcement community. 

Natalia Stankiewicz, CAMS, manager, Financial Crime and Forensic Practice, Deloitte Advisory s.r.o., Prague, Karlín, Czech Republic, nstankiewicz@deloitteCE.com

²⁰ Mazars, “Mazars Central Eastern European Tax Guide 2016,” http://www.taxlink.lv/f/Mazars%20CEE%20Tax%20Guide_2016_web_small.pdf

²¹ Cbonds, “CEE Insights: CEE has been combating tax evasion mainly in retail sector so far,” April 11, 2016, <http://cbonds.com/news/item/823577>

²² Ibid.

²³ Mazars, “Mazars Central Eastern European Tax Guide 2016,” http://www.taxlink.lv/f/Mazars%20CEE%20Tax%20Guide_2016_web_small.pdf

²⁴ Ibid.

²⁵ TMF Group, “How to Close the VAT Gap: An Analysis of the approaches by EU Member States,” July 2016, http://dutcham.hu/datadir/content/highlight/have_337_how_to_close_the_vat_gap.pdf

²⁶ Ibid.

²⁷ Mazars, “Mazars Central Eastern European Tax Guide 2016,” http://www.taxlink.lv/f/Mazars%20CEE%20Tax%20Guide_2016_web_small.pdf

²⁸ TMF Group, “How to Close the VAT Gap: An Analysis of the approaches by EU Member States,” July 2016, http://dutcham.hu/datadir/content/highlight/have_337_how_to_close_the_vat_gap.pdf

Dr. Ali Muhsin Ismail: THE IRAQI FINANCIAL SYSTEM



A CAMS Today had the opportunity to speak with Dr. Ali Muhsin Ismail, governor of the Central Bank of Iraq (CBI), to discuss how the CBI has been enhancing the Iraqi financial system. Dr. Ismail has worked for more than three decades in Iraq, Kuwait and Canada in the fields of management, financial analysis and audit after receiving specialty certificates in accounting, business administration and public finance. In the last 10 years, he took over leading positions. He was inspector general of the Ministry of Oil, secretary general of the Council of Ministers for eight years and is currently assigned as governor of the Central Bank of Iraq.

ACAMS Today: What are some of the steps that the CBI adopted to enhance the Iraqi financial system?

Dr. Ali Muhsin Ismail: The CBI sustains price stability and provides economic activities with a stable path for growth. In addition, it established an effective mechanism to exchange Iraqi dinar with foreign currencies, via the currency window.

Since 2004, the CBI has faced many challenges and has spent a lot of resources, in order to avoid the following bad effects:

- Risk challenges due to bank system weaknesses and financial shallowness
- Dependency challenges—before issuing CBI law (56) in 2004, most of the bank system belonged to fiscal authority
- CBI conducts its monetary policy, in order to re-establish soundness to the banking system

AT: How is the CBI addressing money laundering, terrorist financing and sanctions-related issues?

AMI: The CBI developed an anti-money laundering and counter-terrorist financing (AML/CTF) national strategy for the next five years and it was released in May. This strategy is centered on the following four quadrants:

1. Awareness quadrant: Launch and promote a national media strategy to raise the level of awareness and knowledge of AML/CTF for citizens, government institutions and business organizations, including financial institutions and banks and other related professions. This strategy will depend on effective marketing tools, such as television ads, radio talk shows, posters and newspaper articles to promote the knowledge and understanding of AML/CTF.
2. Restructuring of AML/CTF quadrant: Rebuilding the AML/CTF directorate with a strong emphasis on strong leadership and management, employees' capacity building and talent recruitment program, and implementation of an information technology infrastructure including database, software, hardware and systems, effective and detailed processes and procedures.
3. International coordination and support quadrant: Continue building strong international relationships particularly with the Financial Action Task Force (FATF) and MENAFATF and

corresponding financial intelligence units to share and exchange intelligence, information, and to provide the technical support and assistance needed for knowledge transfer and capacity building.

4. The relationship with local government institutions and private organizations quadrant: Define and improve the relationship with related government organizations, such as judiciary, ministries (trade ministry, taxation and customs office) and intelligence law enforcement agencies and the private sector (banks, financial institutions and related businesses) to promote AML/CTF law, regulations, processes and procedures to counter crimes, terrorism and unlawful financial activities.

AT: What training components are or will be required for professionals in AML/CTF and financial crimes related duties at Iraqi financial institutions?

AMI: We believe that the required training components for professionals working in Iraqi financial institutions are:

- Banks Secrecy Law
- Compliance programs (know your customer)
- Risk assessment programs (AML/the Office of Foreign Assets Control)
- Internal control and monitoring programs
- AML/CTF compliance officer certifications
- AML law integrated into risk intelligence policies and procedures

CBI has started implementing some of these components in 2016 and will continue to deliver others in 2017-2020 by partnering with international professional organizations and external government departments.

AT: Similar to a number of countries in the MENA region, does the CBI envision requiring professionals within financial institutions to hold internationally recognized designations such as the certified anti-money laundering specialist certification?

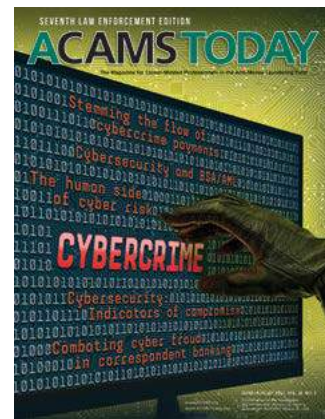
AMI: As any regulated industry such as medical or judiciary and law or education, CBI believes that the financial and banking sector should and must employ professionals with the right qualifications, skills and experience. We have already started implementing standards and regulations for AML, compliance and risk management employees in banks and financial institutions. Therefore, before they are accepted to work at CBI, they must demonstrate these prerequisites. In addition, we have partnered with some reputed international institutions to conduct accredited programs and certifications to ensure that all of our professionals have these credentials. **AI**

Interviewed by: Jose Victor Lewis, CAMS, head of Africa and the Middle East, ACAMS, Miami, FL, USA, jlewis@acams.org

Reading someone else's copy of

ACAMSTODAY?

Join ACAMS and you can receive your own copy every quarter, plus:



- Unparalleled networking with leading professionals in the field.
- Significant discounts on education and training through conferences, seminars, workshops and webinars.
- Professional advancement via ACAMS' worldwide Career Development Center.
- Accreditation as a Certified Anti-Money Laundering Specialist (CAMS), the most globally-respected professional credential in the industry.

ACAMS® Advancing Financial Crime Professionals Worldwide®

For more information and to join contact us by:

Phone +1 (866) 459-CAMS Outside U.S.: +1 (305) 373-0020

Fax: +1 (305) 373-7788

Email: info@acams.org

Online: ACAMS.org ACAMSToday.org

BEYOND DEDICATION: AML PROFESSIONALS IN YEMEN

With each new batch of CAMS candidates that complete the live CAMS training program in Arabic led by ACAMS' training partner, Value for Training and Consultancy (VTC), Khaled Alqubati, the company's general manager looks forward to receiving the CAMS results. As each of the first five candidates from VTC's most recent group sat down this past March at the testing center to take the CAMS exam, it marked the culmination of many hours of studying and preparation all while balancing work-related duties and personal responsibilities. In many ways, the experience for this group of CAMS candidates mirrored that of thousands of anti-money laundering/counter-terrorist financing (AML/CTF) and financial crimes professionals who preceded them, but with one stark and brutal contrast: This group was sitting in a testing center in Sana'a, a city under siege in the middle of a country—Yemen—being torn apart by civil war.

Seemingly, light years from the daily global news headlines about the civil war in Syria, the rise of the Islamic State of Iraq and Syria (ISIS) and the rebuilding of Iraq, the civil war in Yemen is taking place in relative anonymity. According to an article published on March 24, 2017, by the United Nations Human Rights Office of the High Commissioner (OHCHR), since March 2015 at least 4,773 have been killed and another 8,272 injured by the violence. Tragically, "the actual death toll is certainly considerably higher," according to the OHCHR article. Just a few months earlier, in January 2017, the U.N. estimated that around 12 million people were facing famine in Yemen, with 3.3 million people, including 2.1 million children, already acutely malnourished.

As of March 2017, UNICEF reports:¹

- Gross Domestic Product in Yemen dropped by 1/3 from 2014
- Basic commodity prices are 26 percent higher than before the crisis
- The cost of living is now 40 percent higher than pre-crisis levels
- 1.25 million civil servants and their 6.9 million dependents are without an income due to unpaid salaries

The roots of the civil war in Yemen stem back to the Arab Spring as part of a wave of grass roots youth-led uprisings swept across North Africa and the Middle East, dislodging one despot after another along the way. By 2011, the Arab Spring arrived in Yemen and after months of street manifestations and anti-government protests, the country's long-time President Ali Abdullah Saleh was deposed in November of that year in a relatively peaceful departure. Saleh's

vice president, Abd-Rabbu Mansour Hadi, was appointed as his transitional successor and later ran unopposed in a general election to win the presidency outright. Unfortunately, Hadi's time in office was mired by political infighting, a sluggish economy and corruption. In 2014, as Hadi's hold on power waned, a band of militia fighters known as the Houthis, from the northern province of Saada, aligned with former President Saleh and began to expand its foothold in the country through a combination of political negotiations and military conquests. By September 2014, the Houthis entered Sana'a and in January 2015 placed Hadi and his ministers under house arrest. The next month, Hadi escaped to Aden and backed by Saudi funding and weapons, declared the city Yemen's temporary capital. When the Houthis marched on Aden, Hadi fled the country to Riyadh and the civil war entered a new and devastating stage.

Based on the Saudi premise that the Houthi movement represented the Zaidi Shia Muslim minority and that Iran was supplying the rebels with weapons and technical support, Yemen has plummeted into a proxy war between regional archrivals Iran and Saudi Arabia. In March 2015, Saudi Arabia and eight other mostly Sunni Arab states began an air campaign that sought to restore the Hadi-led government. Since then the air campaign along with a naval blockade has continued unabated resulting in a stalemate between the Saudi-led coalition and the Iranian-backed Houthi movement. Complicating matters even further, the power vacuum caused by the civil war in Yemen has served as

¹ "Falling Through the Cracks: The Children of Yemen," UNICEF, March 2017, https://www.unicef.org/videoaudio/PDFs/Yemen_2_Years_-_children_falling_through_the_cracks_FINAL.pdf

fertile ground for the rise of terrorist organizations such as al-Qaeda in the Arabian Peninsula and ISIS.

Stuck in the ongoing crossfire is Yemen's civilian population who struggle to maintain a semblance of normalcy living in a country under siege. It is with this backdrop that Yemen's AML/CTF and financial crimes prevention professionals from both the public as well as the private sectors admirably go about their daily duties to protect their respective financial institutions along with a fragile financial system. "Yemen's financial system is in a very difficult situation, with correspondent bank accounts closed, financial transactions tightened and liquidity tightened," summarized Sadam Abuemran, CAMS, compliance manager at Kuraimi Bank and a member

of the Compliance Managers Committee at the Yemen Banks Association (YBA).

According to Wadie Alsada, head of Yemen's financial intelligence unit, "Financial institutions in Yemen continue to play their normal role despite the challenges posed by the political crisis in the country." Among the challenges, Alsada cites, "Many correspondent banks are reluctant to open accounts for Yemeni banks abroad. This is the biggest challenge facing Yemeni banks as it limits their ability to trade internationally. Many international import activities were halted and other commercial activities were limited to only essential materials and humanitarian work, which reduced the dependence on the services of international correspondent banks, whose work has been covered by the transactions of

Yemeni expatriates." Alsada continued to say, "As a result of increased risks due to the war and political crises, the supervisory authorities increased the level of control and regulatory work on financial and non-financial institutions and the determined professions, which reflected their compliance with AML/CTF procedures. The banks also sought to tighten their systems to face any potential risks." Yet despite these actions, Alsada recognizes how many good customers are complaining about the long time it is taking financial institutions to respond to their inquiries. This, coupled with the lengthy procedures used to fulfill customer due diligence and know your customer principles, is putting great pressure on the customer service departments within the banks to try to balance government regulatory requirements with the retention of valued bank



customers. All of this, in addition to an environment with an economic blockade and hardship and the cessation of salaries is what Yemenis must currently face.

From the perspective of private sector AML/CTF and financial crimes prevention professionals, the civil war and the siege in Yemen has greatly weakened the financial system as the combating parties seek to neutralize the financial system, according to Rasheed Alanesi, compliance manager and head of the Compliance Managers Committee at Yemen Kuwait Bank (YKB). Alanesi recalls how prior to the war in February 2010, Yemen made a high-level political commitment to work with the Financial Action Task Force (FATF) and the Middle East and North Africa Financial Action Task Force (MENAFATF) to address its strategic AML/CTF deficiencies and improve its AML/CTF regime. By June 2014, “FATF determined that Yemen had substantially addressed its action plan at a technical level, including by adequately criminalizing money laundering and terrorist financing; establishing procedures to identify and freeze terrorist assets; improving its customer due diligence and suspicious transaction reporting requirements; issuing guidance; developing the monitoring and supervisory capacity of the financial sector supervisory authorities and the financial intelligence unit; and establishing a fully operational and effectively functioning FIU.”²

While the FATF determined that Yemen completed its action plan in 2014, all subsequent onsite visits to assess whether the process of implementing the required reforms and actions have been halted by the war.

Currently, according to Alanesi, “The military alliance led by Saudi Arabia uses the financial system as a means of blackmail and pressure on Yemenis and the government in Sana’a as part of the

war strategy.” Because of this strategy, Alanesi continues, “There has been a drain on the balances of Yemeni banks abroad by stopping foreign currency transfers to feed banks’ balances with correspondents. Only through international pressure and the international human rights organizations, Yemen is allowed to carry out one balance transfer, which has put many complexities in place. The balances are then deposited with Saudi banks that refuse to transfer the money except to Saudi exporters to purchase Saudi products. Therefore, “the Yemeni financial sector lacks confidence in the Saudi-led alliance. In addition, the internationally recognized government’s decision in September 2016 to relocate the central bank and replace its governor has left the country without an institution capable of providing basic economic stabilization.” Yet another element facing the financial system is the liquidity crisis. Alanesi posits, “Yemen is overwhelmingly a cash economy, and in early June 2016 the CBY [Central Bank of Yemen] began anticipating a liquidity crisis for the domestic currency—meaning that it foresaw itself having insufficient physical banknotes to facilitate normal transactions. Due in large part to the financial blockade on Yemen that prevented the country’s commercial banks from interacting with foreign institutions, traders and wealthy Yemenis had grown increasingly reluctant to let the banks hold their money. As a result, large sums of domestic banknotes were being pulled out of the banking system and held privately, or circulated on the country’s black market. The CBY was not able to print new banknotes because the internationally recognized government was denying the central bank access to the printers, which are located in Russia.”³

Therefore, Yemeni AML/CTF and financial crimes prevention professionals face some truly unique challenges. There is a “proliferation of armed groups [and] the absence of [a] political system in the country” along with “difficulties in identifying illegitimate sources of funds as a result of corruption, bribery, sales of weapons and abduction,” sums up Abuemran. Meanwhile, Alanesi adds, “because of the siege and the reduction of correspondent banks in the world due to the high volume [of] risks, de-risking has become prevalent and the transformation of financial transactions into [the] informal financial system has weakened the AML spirit. This coupled with the inability of Yemeni government specialists to participate in the regional meetings of combating money laundering and the financing of terrorism, especially related to the MENAFATF and ICRG Working Group, and the inability of Yemeni AML professionals to participate in international conferences and seminars as a result of the closure of Sana’a International Airport, has greatly limited and weakened further rehabilitation and training,” according to Alanesi.

It was precisely in this most challenging of environments that the five candidates trained by VTC sat down at the testing center in Sana’a to take the CAMS examination. While the exam is no doubt rigorous and demanding, compared to the environment the candidates faced outside the testing center, it was not overwhelming nor daunting for this group. When the last of the candidates clicked the mouse to submit his exam for final tabulation, the word “pass” appeared on the screen and the last candidate happily joined his fellow newly-minted CAMS graduates. **A**

Jose Victor Lewis, CAMS, head of Africa and the Middle East, ACAMS, Miami, FL, USA, jlewis@acams.org

² “Improving Global AML/CFT Compliance: Ongoing Process,” FATF, February 24, 2017, <http://www.fatf-gafi.org/countries/a-c/afghanistan/documents/fatf-compliance-february-2017.html>

³ Mansour Rageh, Amal Nasser and Farea Al-Muslimi, “Yemen Without a Functioning Central Bank: The Loss of Basic Economic Stabilization and Accelerating Famine,” Sana’a Center for Strategic Studies, September 8, 2016, <http://sanaacenter.org/publications/item/55-yemen-without-a-functioning-central-bank.html>

WHAT IF

you could take the risk
out of reward?

Our comprehensive solutions can help
you manage compliance initiatives - from
strategy through execution.

**At Navigant, we help turn
what if into *what is*.**

Consulting | Outsourcing | Advisory
navigant.com/FinancialServices

NAVIGANT

COMMUNITY BANKING CORNER



Community Banking Corner is a new *ACAMS Today* section that will provide useful tips for Bank Secrecy Act/anti-money laundering (BSA/AML) professionals in community banks to help them in their day-to-day jobs. The Community Banking Corner will focus on all aspects of BSA/AML from de-risking and its effects on smaller banks to efficiencies that can help BSA/AML professionals in community banks. We plan to cover many topics in the *ACAMS Today* magazine and on ACAMSToday.org.


So, if you are a community banker with topic ideas you would like to have discussed, please send them to robert.soniata@bankatunion.com.

Community bankers and working with law enforcement

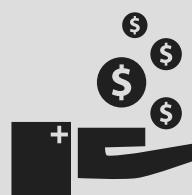
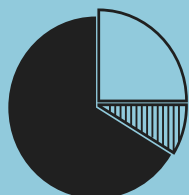
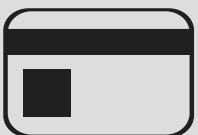
In this inaugural article, on behalf of community bankers everywhere, I want to send a special thank you to the entire law enforcement community for all their hard work and sacrifice to help make the world a safer place.

As a community banker, it is important to make connections with the law enforcement community. From local to federal law enforcement it is essential to be able to reach out to those individuals. Whether it is asking “what if” questions, running scenarios by them or having law enforcement come to the bank to give training, it is an important part of being in a BSA/AML community bank.

In some cases, the communication with law enforcement can lead to better documentation for bankers and better intelligence for law enforcement. It is important to remember as bankers to play within the banking rules while helping law enforcement catch the bad guys.

Making those connections and keeping the communication constant helps both law enforcement and bankers work together to fight financial crimes. 

Robert J. Soniat (Joe), CAMS-FCI, BSA officer, Union Bank and Trust, Glen Allen, VA, USA, robert.soniata@bankatunion.com





KIERAN BEER, CAMS: Telling the important story

A *CAMS Today* spoke with Kieran Beer, CAMS, editor-in-chief and editorial director of *ACAMS moneylaundering.com*, about financial journalism, what challenges financial crime prevention professionals will face in 2017 and one of his favorite quotes.

Beer joined Fortent in May 2006 to launch a new compliance news and legal research, *Fortent Inform*. With Fortent's subsequent purchase of Alert Global Media in January 2007, Beer became editor-in-chief and editorial director of *ACAMS moneylaundering.com*, which incorporated *Inform*, *Money Laundering Alert* and *moneylaundering.com*.

Prior to joining what has become ACAMS, Beer was executive editor of *Bloomberg Wealth Manager*, a trade magazine for financial advisers and family offices. He also served as a staff writer for *Bloomberg Markets Magazine*.

Beer has been a financial journalist for more than 25 years, beginning his career at Institutional Investor, where he worked as a reporter and editor in the newsletter division and was a contributor to *Institutional Investor* magazine. He served as editor-in-chief of *The Bond Buyer*, founding editor of *Thomson Municipal News/The Bond Buyer Wire* and as the editor of the *American Banker*.

Beer writes a column and periodically reports on money laundering and bank compliance. He has served as a panelist and moderator at industry conferences and appeared on CNN, CNBC, WCBS and spoken on NPR and Bloomberg radio (WBRR).

ACAMS Today: What does a typical workday entail for you and what do you enjoy most about your job?

Kieran Beer: My days vary. Sometimes they entail old-fashioned editing or reporting, particularly when our managing editor, Colby Adams, is out or tied up. Other days may involve prepping for something I'm writing or delivering at a conference. To move beyond theory, I block out time to talk with lots of compliance professionals. And, I have a number of management duties. Plus, as a content guy, I am invited to kibbutz on conferences and other areas within the company.

What I enjoy about the job is that I have to learn new things every day, including complex structures for moving illicit funds, how politically exposed persons are buying up London, New York or Vancouver real estate and how geopolitical issues are shaping the latest sanctions from OFAC.

AT: What drew you to a career in financial journalism?

KB: I started out wanting to cover politics—maybe have a column and be a talking head. But I am dedicated to living in New York and there were just so many opportunities in financial journalism. I came to see that financial journalism was as much about telling important stories that involved how people behave and what is at stake in our society as political journalism.

AT: Could you tell us about the first story you reported on or your most memorable story?

KB: Reporters love to talk about how they got that story and I'm no different. As a college editor I got one of my reporters to do a story on discrimination on campus that created change. (The reporter, incidentally, has gone on to be a pretty well-known journalist and documentary filmmaker.) And, when I was just starting out, I did a series on the state of county jails in Michigan for a newspaper with a circulation of 25,000 that became the basis of an argument for better state funding for jails that actually happened. There are too many financial stories to recall, but also early on I learned a lot from a very gossipy story I did for *Institutional Investor* that got picked up by "Page Six" and became a New York magazine feature. The lesson was that neither the "good guys" nor the "bad guys" walk away unscathed from a scandal.

AT: Financial crime prevention professionals face a myriad of challenges, what would you say is the major challenge they will face in the latter part of 2017?

KB: They will have to add new skills to those they already have. We've reported on the increased demand for data analysis skills within AML departments and also about how AML professionals are going to need to work with IT and fraud to fight cybercrime. In the U.S., institutions will need to get ready for FinCEN's CDD requirements and in Europe an ever tougher anti-crime and terror regime from the EU. And, with Fintech on the rise throughout the globe, money can move faster and cheaper and in ways that will present new challenges for compliance professionals to track.

AT: In addition to *ACAMS moneylaundering.com* and now *ACAMS Today*, which ACAMS product or training would you say is one of your favorites?

KB: ACAMS conferences are the best attended in the field and they're exciting places to be to learn new things and to connect to the ACAMS community.

AT: Could you share one of your favorite quotes?

KB: I've thought about what Dreiser says about being a reporter or what E.B. White says about how amazing it is to have a friend who is also a good writer, but I'll go with Mary Ann Evans, aka George Eliot's last lines in *Middlemarch*:

"But the effect of her being on those around her was incalculably diffusive: for the growing good of the world is partly dependent on unhistoric acts; and that things are not so ill with you and me as they might have been is half owing to the number who lived faithfully a hidden life, and rest in unvisited tombs." **TA**

Interviewed by: Karla Monterrosa-Yancey, CAMS, editor-in-chief, ACAMS, Miami, FL, USA, kmonterrosa@acams.org

ADVANCED CERTIFICATION GRADUATES



Aruba

Maria Croes, CAMS-FCI

Barbados

Louis Parris, CAMS-Audit

Canada

Jochen Best, CAMS-FCI

Dwayne King, CAMS-FCI

China

Xiaojie Li, CAMS-Audit

Yanni Mou, CAMS-Audit

Wen Shi, CAMS-Audit

Qian Sun, CAMS-Audit

Zengkai Yue, CAMS-Audit

Hong Kong

Daisy Chan, CAMS-Audit

Al Demeter, CAMS-FCI

Sarika Dhumal, CAMS-FCI

Ka Lai Keane Leung, CAMS-Audit

Oonagh Mckinley-Hutchinson, CAMS-FCI

Kenneth Pemberton, CAMS-FCI

India

Farokh Adarian, CAMS-Audit

Muthukrishnan Balakumar, CAMS-FCI

Poornima Gupta, CAMS-FCI

Laaeth Kumar Mohan, CAMS-FCI

Japan

Toru Sakamuro, CAMS-Audit

Keisuke Suzuki, CAMS-Audit

Masanori Yoshimura, CAMS-Audit

New Zealand

Robert Milnes, CAMS-Audit

Singapore

Rui Jie Terence Ho, CAMS-FCI

Taiwan

Joyce Hsu, CAMS-FCI

United Arab Emirates

Samcy Philip, CAMS-FCI

United States

Pamela Connell, CAMS-FCI

Lindsay Dastrup, CAMS-FCI

Karianne Golemme, CAMS-FCI

Jeannell Graham, CAMS-Audit

Jessica Hughes, CAMS-FCI

Jacob Johnston, CAMS-Audit

Judith Klock, CAMS-FCI

Danielle Kuroski, CAMS-Audit

Sonia Leon, CAMS-Audit

Norma Lopez, CAMS-Audit

Tana Rugel, CAMS-FCI

Kenneth Simmons, CAMS-FCI

Rachel Weygand, CAMS-FCI

FACE THE FUTURE WITH CONFIDENCE

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through a network of more than 70 offices in over 20 countries.

protiviti.co.uk

protiviti®



CAMS GRADUATES: FEBRUARY–APRIL

Albania

Brikena Alliu

Antigua and Barbuda

Candace Wilson

Argentina

Ezequiel Landesman
Enrique Parisi
Carolina Pontoriero
Federico Trucco
Maria Laura Vercellini
Lucia Viola

Aruba

Rachied Habibe
Mayra Janga-Kock

Australia

Conor Hayes
Jin Huang
Bi-Huei Jin
Julie Johannsen
Taehee Kim
Su Peng (Zoe) Lim
Zhanxiang Pan
Ravin Seneviratne
Katharina Shama
Ross Vergopoulos
I Heng Wu

Bahamas

Londena Bethel
April Turner

Bahrain

Hamad Hussain Al Qattan
Ebrahim Afaf
Afaf Ghazwan

Sarah Haider Ali
Syed Ameer Ul Hassan
Yusuf Hubail
Abhilash Keloth
Bushra Abdulwahed Mahdi
Husain Naser

Bangladesh

Pulok Debnath
Mahamudul Hasan
Md. Mahmud Hasan
Mohammad Zabeed Hossen
Md. Amirul Islam
Israt Jahan
Hedayet Ullah Khan
Tania Rafiz Liza
K. M. Lutfur Rahman
Muhammad Ashifur Rahman
ABM Ibrahim Sarwar
Farhana Sumiyea

Barbados

Martyn Del Castilho
Lesah Denny-Brathwaite
Kelvine Jordan-Rowe
Derek Lloyd
Christine Sampson
Tamesha Watkins

Belgium

Mariana Lupascu
Michele Najar
Eleonora Rossi
Marijn van Paassen
Audrey Villance

Bermuda

Heather Kitson
Aisha Mellish

Grace Rogers
Nancy Stevens
Junior C. Watts

Botswana

Catherine K. Moalusi
Theresa Onyadile

Brazil

Michelle L. F. de S. Perfeito
Renato Machado
Artur Morgado
Silvia Rodrigues
Ana Paula Tomé

British Virgin Islands

Judy Anne Juano
Dirk Walters

Canada

Gaspere Abate
Jenette Albanese
Somasundaram Ambalavanar
Reginald Appings
Jessica Bach
Koushikan Bakirathan
Toni Balaam
Eve Belhumeur
Borys Buyniak
Kristin Campbell
Michael Campbell
Thomas Caverly
Brandi Chan
Kathini Cho
Alessand Chou
Cary Chow
Caterina Cuglietta
Elisabeth Danon
Kevin de Bruyckere
Komal Dhillon

Zuwei Ding
David Doumani
Farzana Esmail
David Ferroni
Kathy Galanis
Zeeshan Ghazali
Ekaterina G. Tsimmerman
Ernesto Graveran-Alvarez
Evan W. Green
Fahd Gulzar
Ishita Gupta
Geoff Hermanson
Jeffrey Chih Po Huang
Laeq Ahmad Hussain
Jenny Jones
Stefania Kalogeridis
Tina Kaminski
Daniel R. Kavanagh
Kimberly Kelly
Agnes Kvedraite
Andrew Lanaway
Roderick (Rory) Langran
Shelley Lavalley
Stone Lee
Daniel Lickers-Earle
Ren Liu
Josephine Lofsky
Tuuwala Lok
Amanda Lutchmansingh
Roland Ly
Paula Madulid
Minakshi Maheshwari
Riddhi Mautbar
Don McCrea
Robert McDonald
Hope McKnight
Jeanette McPhee
Nora Mendoza España
David Meunier

Eva Miltz-Theiss
Jerrian Ming
Geeta Mohan
Catherine Moloney
Rakesh Nachnani
Himani Nagrath
Supriya Nair
Bheshini Navaratnam
Alison Ng
Bruce Norgren
Alex Obridko
Aneesh Paranjape
Iryna Pisetska
Chagri Poyraz
Frédéric Prat
Nikhil Puri
Srinithi Raghavan
Stacey Reddick
Ivy Richmond
Jennifer Riordan
Tasha Ruscio
Sumita Sanyal
John Saul
Chris Scheitterlein
Chaitali Senmajumder
Jayashree Seshadri
Gurpreet Sidhu
Krystell Simancas
Jean-Francois Sonson
Ashley Stephen
Alan Tou
Shahidul Waheed
Ruwani Wijesooriya
Tiantian Zou
Juliette Zwarych

Cayman Islands

Javiera P. Aguayo Courbis
Tracia Barrett-Ong
Doreen Brown
Tom Parker

Channel Islands

Liam O'Toole
Hollie Rowe-Roberts

China

Hang Cheong Ao leong
Yuan Chai
Weng Fai Chang
Chanwei Chen
Cynthia Yan Chen
Guorong Chen
Liping Chen
Ruijian Chen
Shuangshuang Chen
Yuwen Chen
Weng Kei Chiu
Szu Chia Chou
Xiaoyun Chu
Rong Dai
Sarah Dan Shao
Xiaofei Dong
Jing Du
Juanjuan Duan
Phoebe Ewen
Xue Fei
Sijia Fu
Wenping Fu
Le Gao
Biqing Guo
Rongyou Guo
Yu Guo
Yun Guo
Ran He
Rong He
Yaosheng He
Yixiao He
Litao Hou
Rongxin Hu
Shan Hu
Qingmin Huan
Caiqin Huang
Eric Ze Long Huang
Qi Huang
Yanling Huang
Peiyi Huo
JiaYan Jian
Hio Man Leong
Guangyu Li
Jian Li
Lan Si Li
Shuang Li
Yuanquan Li
Yupeng Li
Zhaocong Li
Bing Gen Morgan Liang
Li Liang
Mei Na Liang
Jia Wei Lin
Sen Lin
Yi Lin
Li Kun Liu
Lili Liu
Xiao Liu
Yangshan Liu
Wenhao Luo
Zhi Feng Luo
Yao Bin Pan
Xiayun Peng
Miao Qiao
Shuai Qiao
Like Quan
Yan Ren

Xiaofang Ruan
Li Shen
Lirong Sun
Qiao Qing Sun
Jun Tan
Jialiang Tang
Liang Tian
Sok I Tou
Weng Kei Un
Jueyan Wang
Lu (Celeste) Wang
Miao Wang
Midi Wang
Ming Wang
Peng Wang
Qian Wang
Shuyu Wang
Wen Wang
Yan Wang
Wei Wei
Xingtong Wu
Zhixun Xie
Xiaowen Xu
Huifan Yang
Qi Yang
Qianhua Yang
Sen Yang
Yi Yang
Yuchu Yang
Liang Ye
Wu Yin
Xiaohua Yin
Qiyuan Ying
Yao Ying
Yong Yu
Yuan Elaine Yuan
Weilong Zeng
Biao Zhang
Lu Zhang
Meimei Zhang
Xiangyang Zhang
Yan Jie Zhang
Zhiyan Zhang
Kunping Zhao
Shuaishuai Zhao
Yalan Zhao
Shuorong Zheng
Xiaoxiong Zheng
Jiqiong Zhou
Wei Zhou
Xuecen Zhou
Xugang Zhou
Yun Zhou
Zhuoyun Zhou

Costa Rica

Mario Acuña Muñoz

Croatia

Jasmina Cakor
Iva Paden

Curaçao

Denirah Balentina

Cyprus

Yiannos Ashiotis
Niki Charilaou
Lina Hadjifrangiskou
Loukia Matsia
Sophia Nikolatos
Mairita Saulite

Katerina Stephanou

Dominican Republic

Maria Teresa Sesto Feliz

Ecuador

Edwin Rene Aguilar Garnica

Egypt

Abdallah M. M. Abdel Kareem
Aline Aslanian
Amro Mohamed Mounir Taha
Sherif Sabry Youssef Hosny

El Salvador

Inmer Antonio Avalos Baños
Oswaldo A. B. Hernández
German W. Buendía Bonilla
Lourdes M. C. Santamaría
Jose Fernando Castillo Elias
Liliana L. Del Cid Iglesias
Francisco Diaz Barraza
Ricardo Funes Salazar
Gladis del C. H. de Beltran
Juan Jose Hidalgo Amaya
Hugo E. Interiano Melgar
Iliana E. Molina de Villeda
Luis A. Moreno Hernández
Mario A. Orellana Martinez
José Selvin Orellana Sanchez
Carmen E. Pineda de Sosa
Marco D. Platero Paniagua
Dina Patricia Recinos Lemus
Henry Everardo Rivera Padilla
Jorge A. Rodriguez Aguilar
Milton E. Rodriguez Chicas
Carmen E. Rojas de Canales
Carlos E. Torres Vasquez

France

Robert-Michaël Ablin
Pedro Almeida
Wen Sheng Chiang
Julia Colonna d'Istria
Sophie Delgery
Jean Francois Garrick
Julien Huguet
Johanna Lascar
Yasmine Oualhadj
Pierre-Etienne Petit
Haidi Rizo
Rafael Soares Co Rodrigues
Marine Truong
Morgane Tuleau
Patrick Velay
William Zernik

Gabon

Ibath Analor Bikogo

Germany

Aykut Bal
Martina Busch
Sanjukta De
Daniel Denz
Larissa Dethmers
Jakob Diederich
Markus Domeracki
Manuela Drachenberg
Andrea Gaviria
Salvatore Geraci
Holger Hackländer

Simone Heinemann
Patrizia Horn
Andreas Kroeber
Benjamin Kroening
Michael Leifeld
Kerstin Otto
Waldemar Rollheiser
Marceli Rubak
Matthias Stute
Victoria Tessier
Dimitri Trymbach
Dominik Unterein
Linh Vo
Birgit Zahm

Ghana

Naphtali Fordjour

Grenada

Aesia Worme

Guatemala

Vilma I. Marroquin Castillo

Guyana

Karen Chase

Hong Kong

Charity Au
Tak Yin Christine Au
Kit Mei Au Yeung
Chun Man Au-Yeung
Nicole Bossieux
Chun Yip Chan
Hoi Cheung (Samuel) Chan
Kwok Wing Chan
Mei Ling Chan
Parker Chan
Po Yu Chan
Spencer Chan
Sze Wan Chan
Ting Yee Chan
Yau Suen Chan
Cheryl Cheng
Ka Ki (Ally) Cheng
Pui Na Cheng
Ka Kwan Cheung
Ka Lok Cheung
Lok Heng Cheung
Pui Suen Cheung
Shing Pan Cheung
Wing Hung Cheung
Wing Lam (Alyssa) Cheung
Sen Ching
Philip Chiu
Wilson Chiu
Germaine Choi
Siu Ying Chong
Shui Tung Chow
Kim Ki Choy
Angie Shuk Ling Chu
Rebecca Chu
Carol Chun
King Chung Chung
Lai Yin Bell Chung
Xin Duan
Sisi Fan
Richard Farrar
Ka Wai Teresa Fok
Chi Fong
Ki Wing Mabel Fung
Sijin Guo
Ming Kei Hau
Pak Ling Ho
Catharina Hong
Wing Tung Hong
Shifan Hu
Maggie Mei Kwan Hung
Siu Hong Kan
Hoi Yi Olivia Kwan
Ngai Man Kwan
Shuk Ching Kwan
Siu Hei Kwan
Benny Kwok
Choi Har Kwok
Wing Yee Kwok
Chun Kui Kwong
Emily Wai Yee Kwong
Fontane Lai
Myra Lai
Edward Lam
Hoi Ting (Louise) Lam
Yau Chung Lam
Yvonne Ying Tung Lam
Cheuk Yu Lau
Connie Wing Siu Lau
Sik Wang Lau
Yat Fei Lau
Chun Ming Lee
Eric Lee
Flora Nga Lai Lee
Peter Tak Kwong Lee
Roc Lee
Yik Yan Lee
Chun Fung Leung
Chun Yuen Leung
Hoi Ni Leung
Wai Ling Leung
Yan Chi Leung
Chee Kwan Priscilla Li
Chi Shing Li
Jing Ying Crystal Li
Kwok Kiu Li
Ling Ling (Carol) Li
Wai Man Li
Wing Yan Li
Chih Yi Liu
Yanzhao Liu
Man Lung Lo
See Lin Lok
On Ki Angela Lun
Man Wai Ma
Pui Yan Ma
Wallace Chak Keung Mak
Dara Man
Li Hung Mok
Aleksandar Nedevski
Yuen Ki Ng
Yuen Ying Ng
Lo Fan Ngai
Ka Po Nicole Pang
Steve Pang
Chun Man Poon
Yuet Ki Poon
Wenxin Qian
Krishna Rohatgi
Chun Bon Andrew Shiu
Man Fong Sit
Kong Wong So
Wai Sum So
Ching Yi Tai
Ai Wei Tam
Herrick Hei Wai Tam
Lap Hang Chris Tam

Adrian Tang
Cheuk Yiu Tang
Yick Man Tang
Eric Tong
Ho Wai Tong
Timothy Tsang
Wai Ming Tsang
Ka Man Tse
Kai Chi Tsin
Hoi Lun Tso
Cristina Vara
Koon Kui Wan
Xin Wang
Xun Wang
Anthony Wong
Betsy Wong
Chi Wai Wong
Derek Ka Shing Wong
Hoi Ting Wong
Jat Yan Jens Wong
Ka Lai Wong
Ka Yan Wong
Po-hei Wong
Sze Wai Angel Wong
Tsz Ho Wong
Wai Keung Wong
Wan Yi Wong
Wing Sze Wong
Yee Man Wong
Yi Wai Wong
Yu Ho Wong
Yuki Wong
Ka Yan Karen Wu
Yuen Shan Wu
Bingke Xu
Kai Yeow Yap
Philip William Frank Yellen
Chau Ming Ricky Yeung
Chi Fung Yeung
Ka Chai Yeung
Ngai Kwan Yeung
Wai Kin Yeung
Carol Nga Lai Yip
Yui Keung Yiu
Li Ming Young
Xiaohui Yu
Yam Ying Yu
Maggie Yuen
Joanna Dongmei Zhang

Hungary

Tetyana Kausan

India

Sachin Ahuja
Abhishek Bali
Seema Banerjee
Supriya Chandnani
Rajendra Deodhar
Shanthan Gangu
Sagar Ghagre
Krishnan Gopalan
Alok Grover
Subhadra Gundala
Rajeev Gupta
Kiran Hebbar
Jyoti Hegde
Mohammed Ismail
Bharati Jadhav
Jensy John
Swetha Kadam
Santosh Kale

Majo Eyyappan Kanjirathingal
Pardhasaradhi Kasina
Raj Kaushal
Sunil C. Kavishwar
Radhika Krishnan
Tarun Kumar
Manikandan Maruthu
Reema Marwadi
Deepesh Mittal
Saranath N M
Srikanth Nagolu
Nikhil Nanaware
Shikha Negi
Vilas Palanath
Khalid Patharia
Rajyalakshmi Patti
Jayesh Potdar
Aswini Prabha
Saman P. Prabha
Devika Rajadhyaksha
Rajani Ramakrishnan
Leena Ranade
Shilpa Randive
Ranjith Ravikumar
Jugal Ruparel
Arun Satish
Feroz Sayed
Santhosh Sebastian
Urvashi Shandil
Akineth Sharma
Vaibhav Sharma
Virendra Sharma
Monika Shrimali
Anubha Sinha
Vaishnavi Sripriya
Pooja Srivastav
Vipin Thadathil Veettil
Nandhini Thiruvengkatachari
Sunil Thiyyullathil
Praveen V S
Manoj Warrior

Indonesia

Monica (Mona) Adrijani

Iraq

Anas Mohammed Sadeq

Italy

Giuseppe Scampone

Jamaica

Michelle Meek-Davis
Ramonía Swaby

Japan

Toshihiro Amemiya
Yukiyo Ando
Kei Fukuda
Reina Fukushima
Fumiyo Hansell
Risako Hosomi
Kimihiro Imamura
Kazuhiro Kawahara
Takamitsu Kobayashi
Natsuki Kojima
Yu Komuro
Ricky May
Rika Nakaishi
Yukihiro Nakamura
Kiyotaka Niizuma
Yuzuru Nishizawa

Yuji Okumura
Kenji Okuya
Teruyasu Omote
Chihiro Otsuka
Masayuki Sato
Kyoko Shibuya
Hiromi Suzuki
Rie Takeuchi
Hideaki Tanaka
Isao Terada
Sanae Tokita
Hiroshi Yamazaki

Jordan

Maisara Abdullah
Revan Abu Hamad
Nemer Abukaf
Omar Al Jamal
Wameedh Alaa Rasool
Mustafa Al-Afashyeh
Mohammad Al-Fuqaha
Khaled Alnimer
Jude Al-Share
Hiba Ali Hashim Altantawi
Hamza Altork
Marwan Amer Salman
Rafeeq H. Atiyah Al Nashi
Shadi Awwaad
Mohannad Ghaidan
Muna Gharaibeh
Seif Hashem
Mohammad Hawashin
Haneen Thaer Ibadi
Mohammed Tareq Jihad
Dana Khater
Raja'i Musharbash
Soltan Nawras
Mazin Abdulrahman Obaid
Alaa Obaidat
Amjad Shanawani
Samer B. Yousef Muasher

Kenya

Janet Kezengwa
Simion Mwita Maroa
Paul Ngetich

Kuwait

Abdulkareem Al Shaiji
Islam Elsaid Balitta
Atique Ur Rehman Ramzan

Latvia

Linards Anisimovs
Andrejs Bosko
Julija Cukalovska
Aleksandrs Makaricevs
Baiba Preise
Viktorija Ratacova
Andris Rozentals
Svetlana Sidorenko
Gatis Trenko

Lebanon

Lina Ali-Hassan
Hanane Samir Allam
Najwa AL-Makari
Nadine Ghosn Eid
Sarah Badih Hariz
Charbel Hobeika
Hachem Hussein
Hassan Ladki

Elie Moussa
Jad Yared
Nadia Yazbeck
Nizar Zahreddine
Rihaf Zeidan

Lithuania

Indre Dudenaite
Enrika Masalskiené
Greta Mockaityte

Luxembourg

Sonia Garcia
Louis Irelande
Lidia Logutova
Nicolas Marinier
Patrizia Marozzi
Ivana Nesic
Dominik Rohloff
Yin Wang
Alicia You

Macau

Mio Ian Ao leong
Iu Kong Au leong
Fan Bai
Pingping Cai
Chan Wai Chan
Cheng I Chan
Chi Man Chan
Chi Meng Chan
Fong Sio Chan
Ka Wai Chan
Kin Kuan Chan
Kuan Hoi Chan
Man Chan
Sin I Chan
Sio Nga Chan
U I Chan
Weng Tat Chan
Sin I Chang
Kam Man Chao
Son Leng Chao
Ka Ian Cheang
Nga Kun Cheang
Chen Chen
Hanjiao Cheng
Hio Tan Cheng
Wenhao Cheng
Im Seong Cheong
Pek Kei Cheong
Hong Hin Chiang
Cheong Chin Kam
Chi Wa Choi
Sa Lei Choi
Mei Peng Chong
Cheng Kong Chou
Ka Wai Chou
Man Chu
Tak Un Chu
Man Chek Fok
Un Kuan Fok
Sin Wun Fong
Kuan Chan Hao
Chi Keong Ho
Chi Wa Ho
Iok Lin Ho
Sin I Ho
Siu Mui Ho
Ka Hei Hoi
Lok I Hoi
Jinchun Hu

Jingqi Huang
Ying Huang
Yuhao Huang
Man I Ian
Hio Na leong
Sao Chon Io
Ka Man Ip
Chi Vai Iu
In Peng Iu
Meng Hou lun
Yang Jiao
Hao In Kam
Ruilin Kong
Siomui Kong
Sio Un Kou
Cheng Man Ku
Mei Chai Ku
Iam Kuai Chan
Hio Teng Kuan
Pek Lin Kuan
Wa Lam Kuan
Qi Ling Kuang
Pek Ha Kuok
Si Wan Kuok
Un Lou Kuok
Mou Cheng Lai
Sok Yi Lai
Pang Lai San
Chon Ieng Lam
Fong Lin Lam
Ka Cheng Lam
Ka Ian Lam
Sin Man Lam
Wai Ieng Lam
Wai Kam Lam
Weng Hong Lam
Chak Kuong Lao
Ienglam Lao
Wai Hong Lao
Yue Ming Lau
Kuai Mui Lee
Chit In Lei
Ka Ian Lei
Ka Man Lei
Leng Lei
Nga Man Lei
Sio Wa Lei
Wai San Lei
Cheng Leong
Chi Hou Leong
Chi Ieng Leong
Hon Fu Leong
Iok Kit Leong
Iok Teng Leong
Ka Ian Leong
Kam Mui Leong
Lei A Leong
Man Hang Leong
On Leng Leong
Sut Wan Leong
Un Fei Leong
Zhifeng Liu
Chi Leong Lo
In Peng Lo
Ka Weng Lo
Lok Ian Loi
Si Weng Loi
Ka Weng Lok
Vai Man Lok
Kin Ian Lou
Sut Mui Lou
Jiamin Lu

Im Fan Ma
Ka Ian Ma
Oi Ming Ma
Ka Man Man
Lam Man Si
Kuok Chun Mui
long Wai Ng
Ka Meng Ng
Kuan U Ng
Lai Hong Ng
Lai Peng Ng
San San Ng
Sin Ieng Ng
Wai Man Ngan
Pui Fan O
Veng I Pang
Ao leong Pui San
Chi Leong San
Chi Wang Se
Ka Ion Seak
Ruxi Sha
Ka Io Sit
Sok Peng Sou
Nan Sun
Cheok Ian Tai
Kamfan Tai
Chi Fai Tam
In Leng Tam
Sok Ian Tam
Wai I Tam
Weng Ian Tam
Ka Kit Tang
Chi Lek Patricio U
Choi Fong U
Choi Lon U
Chekian Un
Wai Ian Un
Lai I Vong
Sok I Vong
Ranjing Wang
Xiaotian Wang
Yu Wang
Hio Keong Wong
Ka Man Wong
Kai Fong Wong
Kuan Lam Wong
Mei Kei Wong
Percy Wong
Sok Cheng Wong
Wai Peng Wong
Ka Meng Wu
Mei Kuan Wu
Ning Zhang
Zhaohui Zhang
Wenyan Zhao
Xiwei Zhong
Ya Mei Zhou
Fahui Zhuang

Malaysia

Fazleen Azita Abd Rahim
Nur Syafawaty Abd Rahman
Nurizwani Ahmad Zamil
Pushparani Balachandaran
Heng Chee Chua
Gurpreet Kaur Gill
Gladys Goh
Hasaan Hairudin
Syaidah Hashim
Yong-Joon Heo
Lai Yuen Hoh
Chong Wai Hong

Ragunathan Jashvini
Gracelia Jayaseelan
Rulkifli Karpunan
Ik Lee Kho
Yuen Yin (Joannie) Koh
Ho Sang Lee
Suresh Kumar Letchumanan
Tam Huey Li
Ming Lee Lim
Khairul Anwar Mohd Hanifah
Norzurina Mohd Yusof
Mardiana Morshidi
Han Hui Adeline Ng
Soleha Omar
Tomomi Ota
Isan Pang
Raihanna Azrina Roslan
Onkar S. Ludher Sarjit Singh
Muhamad Azhar Suha
Kok Wu Tan
Parameswaran Velusamy
Vinitha Vijayan
Wan M. B. Idlan Wan Bakar
Wong Siow Yee
Belinda Shang Yeh Yeoh
Nadaraju Yoganathan

Malta

Christos Efthymiopoulos

Mauritius

Danielle Ramnuth

Mexico

Jonathan R. L. M. de Oca
Carlos A. Mendoza Romero
Alejandro Nava Leon

Moldova

Oleg Agafonov

Mongolia

Enkhmaa Enkhbat

Montserrat

Rhannon Daley-Williams

Morocco

Ali Mabrouk

Netherlands

Fiyinfoluwa Adeleke
Perry Berkum
Judith Den Hartogh
Kemale Emirbekova
Kevin Kerkhoff
Hans Pijl
Tom van der Woerd
Marie van W. Meijer de Winter
Beini Yang

New Zealand

Phillip O'Leary
Milroy Fernando
Sun Kim
Vik Liu
Ann Marie Olvido
Simon Webby

Nigeria

Ayotola Jagun
Regina Ndaguba

Kingsley Okoeguale
Muhammad Oladipo
Chioma Ossi
Funke Otunla
Oluwapelumi Simpson

Norway

Olivier Audemard d'Alancou
Adis Crnalic
Britt Irene Klubben

Oman

Sabu Vasu

Pakistan

Amim-UL-Ahsan Afir
Irfan Akram
Saad Zikar Jangda
Ali Ahmed Kazi
Saim Mehmood
Muhammad Umer Mughal
Muhammad Zain Siddiqui

Peru

Carlos A. Ludeña Jáuregui

Philippines

Veronica Mae Arce
Jeric Angelo Badian
Rensie Caraig
Haidee Daño
Nancy Dimalaluan
Maria Azalea Echavez
Joanne Michelle Kwan I
Dante Angelo II Ornedo
Sharon Pamplona
Gino Gabriel Rivera
Rayanne Tindoc-Reynoso
Jose Mari Tolentino
Jeffrey Wilford

Poland

Wojciech Cegielski
Jakub Florek
Andrzej Gierasimiuk
Slawomir Jozwiak
Justyna Kudas
Krzysztof Montwill
Skhumbuzo Mwanza
Wei Chien Ooi
Magdalena Paczuska
Dominika Pawlowska
Jan Westphal
Maciej Wodzynski
Matgorzata Wójcik

Puerto Rico

María de Lourdes Jiménez
Luis González Hernández
Diana Ruiz Arvelo

Qatar

Andre Henri Nussbaumer
Chiranjib Parial

Romania

Anda Constantin

Rwanda

Arsene Muhire

Saint Vincent and the Grenadines

Pedro Harry

Samoa

Gafatasi Patu

Saudi Arabia

Sulaiman Al-Dhuwayhi
Ibrahim Aljammaz
Mohammed Almishari
Talal Almuodraa
Saud Almutairi
Saad AlQarni
Mohammed A. S. Al-Subait
Fahad Gormalah Al-Zahrani
Sanjeev Mishra

Singapore

Alejandra Artiguez
Wayne Au Yong
Andrei Bronshtein
Yan Qin Chan
Grace Jok Wei Cheah
Yueh Tung Chen
Shawn Chin
Graeme Docherty
Morgan Fenelon
Ketan Gathani
Sancia Gonsalves
Vikram Gopalakrishnan
Sowmya Gopi
David Han
Vivek Harsh
Prithi Iyer
P. Kalyanasundaram
Yu Ee Francis Khng
Yew Chin Khoo
Oleg Kravchuk
Sulakhana Krishnamurthy
Choi Wai Lai
Hamish Langford
Louie Arch Lantaca
Hwee Chen Lee
Lai Har Christina Lee
Monica Lesmana
Chun Seng Kennedy Lim
Huili Lim
Jiaqi Lim
Joselin Lim
Merri Lim
Wei Ri Lim
Yun Shiuan Lim
Ting Shermaine Lin
Li Chen Loh
Sheena Lye
Thaenarasan M. Selva Rajen
Jose R. Martinez Villalain
Jessie Melinda
Himanshu Naik
Vishal Oberoi
Angela Hui Yan Oh
Abimbolu Olufunwa
Kenny Ong
Firdaus Osman
Pei Ting Pang
Pinaz Patankar
Roopa Patil
Khar Yue Phoon
Tze Yong Png
Ruchira Raj

Gurpreet Rikhray
Yu Hui Jesslyn Seah
Kah Lim (Louis) Seah
Vivek Seth
Puay Khim Sia
Mun Kian Siew
Doris Soh
Chris Stark
Cai Quan Tai
Rubal Talwar
Esther Li Lin Tan
Hui Kiow Tan
Kian Boon Tan
Mark Khai Shean Tan
Rachel Jui Ying Tan
Rui Zhi Ray Tan
Shujuan Evelyn Tan
Xue Min Tan
Zhong Lun Tan
Choon Yong Teo
Dominic Wei Luo Teo
Grace Hui Boon Teo
Lily Teo
Rachel Teo
Cenwei Toh
Michelle Trinidad
T. Vijayakumar
Victoria Wade
Norhasikin Wahid
Brian Wong
Hai Mei Wu
Jialong Yap
Lorraine Yeak
Shiqi Zhu

Sint Maarten

Thomas Riemersma

Slovakia

Tamas Svab

Slovenia

Tomaz Ogorevc

South Africa

Barend Badenhorst
Alida Botha
Natalie Bowman
Nazeefa Cassim
Colette de Villiers
Elanie de Vries
Ryan Jude Desai
Shaun Els
Nicki Koller
Christiaan Lubbe
Rhadika Maharaj
Mamokhatla Mayinga
Monique Milligan
Alistair Naidoo
Bradley Rae
Amit Ramiez Dayal
Vicki Robinson
Michelle Sewchuran
Dan Wu
Lwazi Zaca

South Korea

Sung Ok Min
Yoon Sang Seong

Spain

Jesús Campos Poveda

Helena Cebrián Benito
Maria C. de Antonio Carballo
Cristina Rodríguez Visus

Sri Lanka

Nathasha Gajadeera
Gayana Perera

Sweden

Madeleine Hampson
Håkan Hartzell
Christian Wandt

Switzerland

Jenny J. Choi
Henry Konsén
Oriana Steiner
Claudio Zatta

Taiwan

Jen Chun Chai
Tsung Shien Chan
Chihchieh Chang
Chin Ming Chang
Li Chun Chang
Mei Hui Chang
Sheng-Fa Chang
Tien Cheng Chang
Ya Fen Chang
Yen Mei Chang
Yu Ching Chang
Yu Ling Chang
Wei Chao
Wen-Hsiu Chao
Yung-Hsi Chao
Chia Hao Chen
Ching I Chen
Hsiao Chieh Chen
Hsin Chu Chen
Hsin Yi Chen
Hsin-Wen Chen
Hui Ju Chen
Hung Jen Chen
Hung-Hui Chen
I Hsin Chen
I-Chen Chen
Jen Huei Chen
Jhong Wei Chen
Josephine Chao Jung Chen
Kuan Jen Chen
Kuo Pao Chen
Ling Chen
Mei Ya Chen
Min Chuan Chen
Po Hsi Chen
Shu Wen Chen
Tai Ming Chen
Tian Fu Chen
Ting Fang Chen
Weiting Chen
Wen Hsin Chen
Wen Man Chen
Yen Shan Chen
Yi Chen Chen
Yi Chun Chen
Yi-Chieh Chen
Ying Fang Chen
Yu Ling Chen
Chien Ju Cheng
Yu Jung Cheng
Yu Yu Cheng
Yun-Hsuan Cheng

Ho Chia Ying
Ching Yi Chiang
Pei Chun Chiang
Cheng-Hui Chou
Hung-Chang Chou
Lo Wei Chou
Yu Chuan Chu
Wan-Ju Chuang
Yi Chia Chuang
Yang Hsuan Fan
Shih-Wen Feng
Su Wan Feng
Yun Ting Gao
Hui Ru Gau
Hsin Pei Ho
Tzu Ying Ho
Yan Jun Hong
Jen Wei Hsiao
Cheng Han Hsieh
Emy Hsieh
Kun Yu Hsieh
Lie Yu Hsieh
Peng Hsiang Hsieh
Wan Chun Hsieh
Chang Yi Hsu
Chia Chi Hsu
Guang Yu Hsu
Hui-Tien Hsu
Kai Ting Hsu
Kou-Chih Hsu
Nai-Yi Vicky Hsu
Ruei-Yu Hsu
Tshui Hsu
Wei-Min Hsu
Su Jane Hu
Cheng Hang Huang
Chi Kuei Huang
Chi Min Huang
Ching Chuan Huang
Ching I Huang
Ching-tse Huang
David Huang
Kuo-Hua Huang
Mei-Tzu Huang
Shr Hang Huang
Tien Fu Huang
Pei Ling Hung
Ya Ting Jhang
Pei Sian Jhu
Ning Yang Kao
Chen Wei Ku
Chia Hsuan Ku
Chu Chih Kuo
Chung Chien Lai
Tzu Jung Lai
Tzu Hsuan Lan
Hui Ling Lee
Jeremy Yen-Ming Lee
Shiuan Rung Lee
Su Hui Lee
Wei Min Lee
Yuan Ting Lee
Fu Kai Lei
Ching Ming Leu
Hsiao Chuan Li
Tzu Yu Li
Chia Chi Liang
Chien Chi Liao
Hsin Yi Liao
Lung Chi Liao
Pei Lin Liao
Tzu-Yao Liao

Yvonne Lien
Ching-Sheng Lin
Hsin I Lin
Hsin Yi Lin
Hsiu Chou Lin
Huan Wen Lin
Hui Min Lin
I Chun Lin
I-Ling Lin
Jia-Rou Lin
Jiun Jaan Lin
Jo Wen Lin
Kai Wen Lin
Kimberly Yu Tzu Lin
Liang Yi Lin
Pei-jung Julia Lin
Tony Yu Hung Lin
Tzu Chao Lin
Xin Yan Lin
Yi Hsiu Lin
Yih-Ming Lin
Ying Chih Lin
Yu Cheng Lin
Yu Chuan Lin
Yu Ju Lin
Yuan Chang Lin
Dung-Yan Kenny Liou
Chia Yu Liu
Huai Te Liu
Louis Che Wei Liu
Shu Min Liu
Wei Chen Liu
Yi-Chang Liu
Yun Wen Liu
Hsiu Huan Lo
Ying-Tsung Lo
Yu Jen Lung
Hsin Yi Pai
Ti Pang
Ling Ya Su
Tracy Siou Ya Su
Vanessa Su
Huang Szuyao
Ke Wei Tai
Yung Sin Teng
Hui Min Tsai
Juyu Tsai
Kang Shui Tsai
Po-keng Tsai
Shih Hao Tsai
Shu Han Tsai
Shueh-Yun Tsai
Wu Hsin Tsai
Yen Ting Tsai
Chen Jung Tsao
Yu An Tsao
Lin-Ping Tu
Cheng Hua Tuan
Ho Yun Chris Wan
Tsen Wan Wan
Hui Chih Wang
Kuang-Tse Wang
Kwo Chin Wang
Michelle Mei-Wen Wang
Ping-Han Shirley Wang
Wan Yi Wang
Yichen Wang
Yu Hsuan Wang
Yu Ting Wang
Ling Chun Wen
Min-Chiao Wen
Chia Chien Weng

Chia Fang Weng
Wen Jin Wroun
Ai Hui Wu
Cheng Ping Wu
Chih-Hsin Wu
Guan Shiun Wu
Vivienne Wu
Wei-Cheng Wu
Pan Xuan-Yu
Mingfen Yang
Sheng Hsun Yang
Yu Shiuan Yang
Teng Han Yau
Chi Min Yeh
Hui Wen Yeh
Chun-Yi Yen
Shau-Ling Yen
Pei Thu Yo
Chang Ruey Yu
Li Yueh Yin

Thailand

Shain Ren Chen
Li Chun Chien
Yi Tsou Liu
Vipada Luppayaporn
Chayawat Sattabusya
Peerapong Sophaariyanant
Chi Wei Tsai

Trinidad and Tobago

Janelle Bernard
Sharlene Dabideen
Sabrina Lee-John
Karla Simmons

Turkey

Melike Esin Etiler
Nazli Ipek Tuzun

Turks and Caicos Islands

Yesicha Robinson

Uganda

Ssenyondo Godwin

Ukraine

Kostyantyn Mukhlygin

United Arab Emirates

Ghulam Abbas
Hany M. Shawky Ahmed
Sohail Akbar
Charanjeet Singh Bhatia
Po-hsun Chang
An Shun Cheng
Jaffrie Cherian
Lesley Ann D'Souza
Michelle Fernandez
Tamer Ghresi
Manish Gupta
Swati Jhanb Roy
Muhammad Zahoor Khan
Nadim Kourda
Nikita Lihala
Aijaz Hussain Mohammed
Khalid Nadim
Pradeep Nair
Imran Noor
Sabu Pallithazhath
Moiz Patel

Sajith Peiris
Annum Rai
Syed Saeed
Ali Seghir
Suchit Piyush Shah
Ramesh Shaw
Peng Shi
Srividya Sreedhar
Sanjeev Srivastava
Hozefa Suratwala
Rudolf Tison
Aqeela Umer
Sara Wahba

United Kingdom

Ali Abiri
Idowu Adelaja
Ibrahim Adetona
Hakeem Agaba
Kaleem Bajwa Ullah
Mike Banka
Brooke Bear
Stephen Blackburn
Lucy Callaghan
Josie Carnie
Anastasija Cerniavskaja
Josef Charles
Neeraj Chopra
Helen Crockett
Bruce Duff
Emma Dwyer
Amira Egala
Olivia Goldberg
Lindsey Gordon
Edmund Hughes
Raja Hussain
Roeland Huyskens
Colin Johnson
Tim Jones
Sunil Kalagara
Muhammad Kashif Khan
Kirshan Lal
Peng Liu
Sanhita Majumder
Nisha Malik
Dolores Martinez Aguirre
David Mawdsley
Alison McCaffrey
Neil McCappin
Patrick McLean
Subha Mohan
Kaspars Muiznieks
Candice Mullings-Adeniji
Anna Nomerkova
Cian O Larkin
Oyinlola Ojo
Adewole Olufon
Alex Osagie
Idehen Osagie
Deepak Patel
Andrew Pennock
Melissa Percy
Carlo Portelli
Rebecca Ramsdale
Joshua Rawcliffe
Rose Reynolds
Sam Riches
Astrid Rouleau
Mina Sawieres
Hiu Yu (Catherine) Shen
Nitin Singhal
Hasham Tahir

Garry Ting
Induvant Tomar
Amnon Trebish
Dritan Vakaj
Sebastiaan van Nooten
Naresh Vanniyasingam
Vanessa Vaz
Neeraj Verma
Vincent Viney
Alfred Waithaka
Matthew Winters
Haifeng (Kevin) Xie

United States

Ahmed Abdelnabi
Katrin Abougnima
Percy Abraham
Carmen Abreu
Mechile Adams
Ross Adams
Valina Addo
Mustapha Adelekan
Matthew Adkins
Jonathan Adler
Veronica Adorni
Madhu Sudan Agrawal
Tanvir Ahmad
Olayinka Ajakaiye
Rajesh Aji
Nicholas Albini
Joseph Alemu
Daniel Alexander
Sadik Alimov
Gregory E. Allen
Samuel Allen
Gerald Allora
William Alverson
David Ambrose
Dean Amer
Rosalin Andres
Melissa Andrus
Gina Aquilia
Jeffrey Aquino
Emma Arizpe
Tara Armendariz
Paul Aversano
Alba Avila Quintana
Paul Avinger
Tanja Bacic
Michael Baer
Mark Baker
William Bakshi
Shantel Barragan
Chelsea Bartley
Cassandra Bates
Alissa Bell
Bethany Benesh
Cristian Bennett
Christopher Benton
Carlos Betancourt
Lauren Beyer
Aditi Bhardwaj Pascual
Vinish Bhatia
Alexander Billak
Brad Birkholz
Josh Blizzard
Matthew Bloom
Franziska Blunck
Peter Bogomol
Aaron Bolder
Angela Bond
Michael Bonnier

Tatsiana Bookbinder
Artin Borjas-Moreno
Kristy Bower
Abigail Boyd
Brad Boyken
Alana Boyle
Gustavo Brandao
Kiki Brannan
Steven Breen
Seth Bridge
Bradley Brock
Edward Brooks
Genesis Bryan
Amanda Bryant
Bryan Bulat
Tara Burch
Karla Burks
Zach Bush
Bernard Butler
Evelyn Butler
Michael Butler
Nathan Buttleman
Shannon Buzzerio
Mary Byrd
Ingrid Byrne
Xun Cai
Jason Calvert
Stephen Cameron
Kayla Campbell
Steven Campbell
Michael Campites
Christine Canute
Patrick Cappel
Nicholas Caputo
Corey Cardoza
Vincent Carpio
Nancy Case
Benedict Castro
Debra Catarozoli
Kelly Cervantes
Heather Chakan
Jignesh Chande
Kartik Chaudhary
Anne Chen
Da Chen
Jay Chen
Yi Cheng Lu
Robert Cherofsky
Liyang (Lena) Chiang
David Cho
Nicholas Cho
Rita Choudhury
Sreeradha Saha Choudhury
Obianuju I. Chukwuana
John Cino
Joseph Clemente
Brent Close
Elyzabeth Colan
Bobbie Cole
Alan Coleman
Jennifer Collins
Rocco Cononico
Denise Conrad
Bradley Coppella
Shawna Corder
Dana Cordes
Janice Costa
Sharon Coté
Tara Cowan
Valerie Craft
Stephen Cress
Andrea Crittle

Christopher Crovatto
Thelma Cudjoe
Daniel Cunningham
Diana Cunningham
Sean Cunningham
Clinton Dalton
John Daly
Jordan Dant
Thomas Dapp
Iszellyn David
Tammy Davis
Tyrone Dawson
Luke de Araujo
Parisa de Neree T. Babberich
Jeffrey J. DeChristopher
Alexander Deligtisch
Judith Derenzo
Kirsten Derynioski
Stephanie DeZarn
Gina DiGiammarco-Ridge
Galin Dimitrov
Rodica Dingess
Nancy diSibio
Brandon Dombrowski
Tracy Donahue
Jeremiah Dort
Marcia Douglas
Amanda Dowling
Philip Dragotta
Meghann Duerfahrd
Mudit Duggal
Paxton Dunn
Elizabeth Duran-Vargas
Chris Dylla
Jeanne Eastman
Ed Edmister
Bruce Emory
David Epps
Robert Erdogan
Shannon Escalante
Elizabeth Eschbach
Michael Estevez
Silvy Evans
Eric Facuri Petrarca
Mark Farmer
Shirley Fiano
Justin Fields
Michael Finkelstein
Isaac Fisboin
Mark Fitzgibbon
Joshua Fogel
Dee Foster
Steven Foster
Shona Frain
Charles C. Francis
Maria Frates
Jessica Freeland-Ahrens
Corey Freynik
Bert Friedman
Jessica Frith
Karl L. Fromm
Mayra Fuentes
Carlos M. Fuentes Salinas
Dominick Gaetano
Nicholas Gaffney
Peter Galop
Maxim Galperin
Trupti Gandhi
Tyson Garbrecht
Vladimir Garcia
Rajeev Garg
Victoria Garrod

Sibi George
Christopher Gibson
Dana Gilbert
Lorenzo Giulianotti
Kristy Glassen
Jonathan Gold
Charles Goldstein
Carlos Gonzalez
Jeffrey Gonzalez
Stephen Gonzalez
Neil Goradia
Arlington Gordon
Keisha Gordon
Taylor Goss
James Gothe
Kay Goudey
Jennifer Gray
Kyle Grella
Amy Grove
Amanda Grube
Srinivas Guduru
Brad Gushiken
Cesar Gutierrez
Misato Hafez
Sayoni Haldar
Megan Hall
George Hamje
Kathy Hart
Michael Harvey
Lea Harvin
Cory Hauser
Michael Hayden
Lucy Hayrabedian
Molly Heath
Raymond Heinrichs
Anna Helle
Kevin Hellman
Edgardo Hernandez
Jose Hernandez
Judd Hesselroth
Carolyn Hill
Randolph Hobbs
Ashley Hodges
Erjola Hodo
Kevin Hoffman
Nicolas Holch
Seanne Holliday
Joanne Holt
Claire Holtzmuller
Connie Hooks
Cindy Horton
Anne Howard
Howard Hull
Daron Hunt
Kathleen Hunt
Ana Iacovone
Mike Idol
Ellen Iggulden
Stefano Illiano
Saul Infante Fernandez
Hope Inouye
Elvanelga Isernia
Haruya Ito
Omar Jadan
Adrian Jaimes
Jason James
Carissa Janowiak
Nikki C. Jarrell
Chad Jeckel
Susan Jennis
Sandra Jensen
Aimee Jess

Sandy Jeyaraj
Vishal Jhagadiawala
Adam Jhugdeo
Lilin Jin
Jacqueline Johnson
Joni Johnson
Bryan Jones
Christopher Jones
Julie Jones
Ravikanth Jonnalagadda
Guy Jopling
Andrea Joson
Tammy Jung
Shaina Jusino
Bryan Jones
Alex Katsaros
Stavros Katsetos
Brian Katz
Harpreet Kaur
Claudia Kaushik
Meenakshi Kaushik
Kelly Keen
John Kelleher
Harvey Kelly
Scott Keppel
Nitesh Khanna
Evgeniya Khilji
John Kim
Lance Kinzle
Judy Klare
Yulia Klimov
Antonio Knox
Jacqueline Ko
Cristina Koder
Jenny Kofman
Richelle Koontz
Prajakti Kotwal
Alan Kravit
Roman Kucherak
Samuel Kuehn
Ryan Kuklinski
Carl Kunz
Samuel Kusewicz
Carrie Kwok
Jeannie Kwong
Matthew La Salle
Jeremiah Lahnum
Andrea LaMothe
Patrick Lampart
William Land
Monique Lang
Charles Lansdown
Victoria Large
Patricia Latella
Linh Lau
Charlie Laurence
Christopher Layfield
Bao-Kim LE
Mary LeBeau
Elise Lebourg
Aspen Lee
Ellen Lee
Hsin Ju Lee
James F. Lee
Ming Bun Lee
Samantha Lee
Stephen Lee
Tae Yeon Lee
Colette Lesperance
Kimberlie Lewin
Annie Liao
Lee Feng Lin-Cheng

Deborah Lincoln
 Ronald Link
 Phillip Liu
 Yi Liu
 Elle Lockett
 Nathalie Lonsdale
 Lucia Lopez
 Florian Lorenz
 Kevin Loria
 Sandeep Loshali
 Carrie Luman
 Boris Luzhansky
 Michael Lynn
 Joseph Mader
 Andrew Magas
 Hina Mahmood
 Marlyn Maisonet
 Christopher Makowski
 Steve Malerba
 Andres Mancheno
 Prateek Manek
 Petronela Manescu
 Elisia Marcelino
 Blake Marino
 Norman Mark
 Jill Markus
 Tom Maroney
 Liz Marquez
 Brandon Marshall
 Michael Marshall
 Nicholas Marsini III
 Nicholas Marsit
 Janine Martin
 Joel Martin
 Larissa Martin
 Louis Martinez
 Stephanie Martinez
 Hilary Marx
 Shara Mason
 Jeffrey Mayausky
 Lance Mayberry
 Patricia McCallop
 Colin McCormick
 Frank McDonagh
 Thomas McIntosh
 Jared McJunkin
 Melissa McLaughlin
 Bruce McLean
 Mark McNulty
 Tara McSorley
 Eric Medoff
 Kristen Meehan
 Robin Meerkatz
 Jennifer Melendez
 Marsha A. M.-Beersingh
 Daniel Merrell
 Amy Mesenbrink
 Lisa Metzger
 Nicholas Meyer
 Lee Matthew Minervini
 Haszliyana Minhad
 Lourdes Miranda
 Jonathan Misskerg
 Pratti Rama Mohan
 Karen Moloney
 David Monderer
 Kelly Montanaro
 Damon Monterrubio
 Jessica Monteux
 Yericca Morales
 Robin Moran
 Miriam Morris
 Annette Morrison

Nicole Moser
 Steven Mowery
 John Muir
 Gabrielle Murphy
 Ashley Murray
 Cassandra Muscat
 David Mustar
 Melanie Myint
 Rana Nahr
 Jayakrishnan Nair
 Michael Nakis
 Yountae Nam
 John Napoleon
 Stasis Nelaimischkies
 Amy Nelson
 Rao Nemani
 Deyquan Nesbit
 Todd Newall
 Chi Ngo
 Aurora Nieves
 Natacha Noguera Marron
 Jessica Nolan
 Stacy Norton
 Venkata Nuthakki
 Brittany Nye
 Robert Obayda
 Matthew O'Brien
 Adam O'Connor
 Schylur M. O'Doherty
 Styve Ogando
 Mercedes Olivares
 Patti Oliveira
 Robert Olszewski
 Ama Osei-Boateng
 Jianyu Ou
 Rose Pagan
 Mahesh Pai
 Edgar Paiz
 Steven Pak
 Ronald Palais
 Andreea Panfiloiu
 Cody Pannella
 Larry Parham
 Anita Parker
 Jonathan Parks
 Paulo Parras
 Sharon Pasquarelli
 Bhavin Patel
 Tina Patel
 Vishal Patel
 Valerie Patterson
 Dean Paul
 Ashley Penn
 Sonia Pereira
 Ashley Perezluha
 Lisa Perfetti
 Georgennia R. Peschke
 Monique Peterson
 James Petraglia
 Sarah Petrosch
 Matthew Phillips
 Clint Philpot
 Patricia Piche
 Crystal Pinthong
 Anita Piper
 Diane Pisacreta
 Christopher Plath
 Kevin Polansky
 Jose Porrata
 Richard Postiglione
 Karrie Prehm
 Christina Prevot

Alyssa Procopio
 Antoinette Prokopczyk
 XiLing Qian
 Zeeshan Quadar
 Katharina Quintus
 Jacqueline Quintyne
 Eric Radue
 Fara Rosalind Rajkumari
 Jaime Ramirez
 Trisha Ramirez
 Richard Ramon
 Elvin Ramos
 Marisa Rampersad
 Christopher Ramsey
 Kiran Rane
 Heather Ransom
 Angela Ratliff
 Shishir Rawat
 Rashada Reddick
 Chantell Redish
 Jeff Reed
 Thomas Rees
 Christopher Rehberger
 Denise Reske
 Keron Reyes
 Richard Reynolds
 Charles Rho
 Denice Richarts
 Luz Rios
 Jolene Rizk
 Ezequiel Roa
 Benjamin Robey
 Jessica Robinson
 Aivanett Rodriguez
 Antonio Rodriguez
 Juan Carlos Rodriguez
 Michael Rolsch
 Connie Romay
 Chenyuan Rong
 Anthony Rooney
 Kathryn Rosa
 James Rossiter
 Romita Roy
 Alicia Ruiz
 Sergio Rumayor
 Timothy Rusavuk
 Sara Russel
 Judith Russell-Dookan
 Jonathan Russolese
 Marisa Ruthven
 Alexandra Sagaro
 Nancy Salgado
 Mindy Salvati
 Rolls Sam
 Laura Sammon
 Sam Samuel
 Paola Sanchez
 Michael Sandretto
 Juliet Sardiñas
 Lauren Schick
 Kristina Schilling
 Cassie Schock
 Dana Schwartz
 Svetlana Schwartzman
 Jennifer Scotland-Lyle
 Lea-Ellan L. Scott
 Ryan Scott
 Vineet Sehgal
 Riaz Shaik
 Yaniv Sharabi
 Mahyar Shariati
 Puneet Sharma
 Lisa Shea

Stephanie Sheehan
 Abiy Sheferaw
 Kelly Sheffield
 Tim Shepard
 Thankie Shi
 Helen Irene Shippee
 Miroslava Sikurova
 Andrew J. Simone
 Robert Sinex
 Hemlaxmi Singh
 Keshav Manmohan Singh
 Suvarna Singh
 Amanda Slavin
 Devin Smith
 Latoya Smith
 Patrick Smith
 Tyler Smith
 Monica Snider
 Jeong So
 Thomas Sofia
 Cherie Soto
 David Specht
 Carmine Spinelli
 Jason Stanley
 Kevin Stefani
 Jonathan Steffy
 Michelle Stein
 Paul Steinmyller
 Peter Steltz
 Khushali Stepnowski
 Tatjana Stojanova
 Jeron Stonehocker
 Melissa Stover
 Spencer Stowell
 Ryan Streicher
 Peter Strobel
 Toneta Sula
 Mallory Sun
 Yi (Jenny) Sun
 Christopher Susskin
 Justin Svec
 Madina Tahiry
 Michelle Tavares
 Sara Taylor-Chanez
 Laura Teasley
 Bruce Temple
 Anita Thomas
 Patrick Thomas
 Lawrence Thompson
 Eva Thorpe
 Graham Todd
 Andrew Toensmann
 Joshua Tolbert-Smith
 Karlo Torres
 Barry Towle
 Cordia Tucker
 Michele Upshaw
 Julie Van Paassen
 Eldon Vaz
 Mariela Vazquez
 Cecilia Velazquez-Chavez
 Peggy Vering
 Andrea Vidaurre
 Michael Villeda
 Jenna Voss
 Angela Wagner
 Craig Wagner
 Charles Waikwa
 Dennis Walker
 Guenevere Walker
 Keith Walker
 Melissa Walker

Thomas John Walsh
 Jasman Walson
 Huatian Wang
 Nicolas Wart
 Christopher Watkins
 Chandler Wavro
 Edward Wegener
 Toni Weirauch
 Michael Wenner
 Kurt Wessel
 Careisha Whyte
 Annika Wiese
 Brianys Wiggins
 Deborah Wiley
 Harley Williams
 Calena Willingham
 Kristin Wilsey
 Kassondra Wilson
 Stephanie Winegarden
 Jennifer Winkles
 Ashley Wisdom
 Randall Wodicka-Cudey
 Kelly Wong
 Youn Ju Woo
 James Woolnough
 Rachel Workman
 Heather Wright
 Long-Long Wu
 Meelder Wu
 Yu Fei Wu
 How Bee Xan
 Andriy Yahniuk
 Shintaro Yamabe
 Saathi Yamraj
 Kristie Yang
 Michelle Yarrow
 Marianne Yen
 Alexanne Yi
 Michelle Yong
 Alyssa Young
 Tatyana Zabrovskiy
 Homam Zaini
 Nella Zelensky
 Youwen Zhang
 Christine Zieminski
 Amy Zimmerman
 Estefanie Zurita

Uruguay

Rodrigo Pagliaro Ieritano

Vietnam

Linh Nguyen
 Pham Trang

Yemen

Sadam Abduh AL-Sofi
 Mohammed Hassan
 Farid Mohammed Mamon
 Mohammed A. S. Albakelee

Zambia

Velika Mpundu

Zimbabwe

Tichafa Chigaba
 Casper Chimutsa
 Nyaradzo Chiwewe
 Clara Hwata
 Tongesayi Murape
 Kenneth Ngwarai

Why spend 3 days with some of the brightest minds in AML audit or financial crimes investigations?

To earn the recognition you deserve for committing to protecting and elevating the status of your institution.



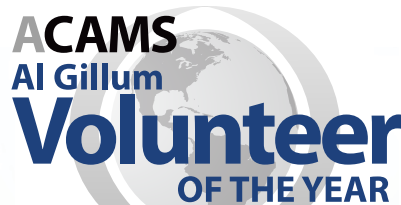
Earn the most exclusive and distinguished designation beyond CAMS that ACAMS offers. Email advancedcertification@acams.org to get started.

AML and Financial Crimes Professionals with ACAMS Advanced Certifications* are recognized as elite seasoned professionals with superior skills committed to and focused on growing professionally to benefit their institutions.

*You must be CAMS Certified in order to apply.



2017 **ACAMS** RECOGNITION AWARDS



SUBMIT YOUR NOMINATIONS AT:

<http://www.acamsconferences.org/vegas/awards/>

Submission Deadline is July 28





